Ficha temática

PROTEÇÃO DOS DADOS PESSOAIS

O direito à proteção dos dados pessoais é um direito fundamental cujo respeito é um importante objetivo para a União Europeia.

O referido direito está consagrado na Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta») que dispõe no seu artigo 8.°:

«1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.»

Este direito fundamental está além disso estreitamente relacionado com o direito ao respeito da vida privada consagrado no artigo 7.° da Carta.

O direito à proteção dos dados pessoais também está previsto no artigo 16.°, n.° 1, do Tratado sobre o Funcionamento da União Europeia (TFUE), que a este respeito sucedeu ao artigo 286.° CE.

Quanto ao direito derivado, a partir de meados dos anos 90 a Comunidade Europeia dotou-se de diferentes instrumentos destinados a garantir a proteção dos dados pessoais. A Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [1], adotada com base no artigo 100.°-A CE, constitui o principal ato jurídico da União nesta matéria. Esta diretiva prevê as condições gerais de licitude do tratamento desses dados bem como os direitos das pessoas em causa e prevê, nomeadamente, a criação de autoridades independentes de fiscalização nos Estados-Membros.

1 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281, p. 31), versão consolidada em 20.11.2003, revogada a partir de 25 de maio de 2018 (v. nota 5).

Em seguida, a Diretiva 2002/58/CE [2] veio completar a Diretiva 95/46/CE, procedendo à harmonização das disposições da legislação dos Estados-Membros relativas à proteção do direito à vida privada, nomeadamente no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas [3].

Além disso, no âmbito do espaço de liberdade, segurança e justiça (ex-artigos 30.° e 31.° do TUE), a Decisão-Quadro 2008/977/JAI [4] regulamenta (até maio de 2018) a proteção dos dados pessoais no domínio da cooperação judiciária em matéria penal e policial.

A União Europeia elaborou recentemente um novo quadro jurídico geral nesta matéria. Para o efeito, em 2016, adotou o Regulamento (UE) 2016/679 [5] sobre a proteção de dados, que revoga a Diretiva 95/46/CE e que será diretamente aplicável a partir de 25 de maio de 2018, e a Diretiva (UE) 2016/680 [6] que visa a proteção dos referidos dados em matéria penal, que revoga a Decisão-Quadro 2008/977/JAI, e cujo prazo de transposição pelos Estados-Membros foi fixado em 6 de maio de 2018.

Finalmente, no contexto do seu tratamento pelas instituições e órgãos da União, a proteção dos dados pessoais é assegurada pelo Regulamento (CE) n.° 45/2001 [7]. Este regulamento permitiu nomeadamente a criação, em 2004, da Autoridade Europeia para a Proteção de Dados. Em janeiro de 2017, a Comissão apresentou uma proposta [8] de um novo regulamento que revoga o Regulamento n.° 45/2001 e a Decisão 1247/2002/CE e que visa modernizar as regras na matéria bem como alinhá-las com o novo regime estabelecido pelo Regulamento (UE) 2016/679.

2 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (diretiva «Vida privada e comunicações eletrónicas») (JO L 201 de 31.7.2002, p. 37), versão consolidada em 19.12.2009.

3 A Diretiva 2002/58/CE foi alterada pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO L 105 de 13.4.2006, p. 54). Esta diretiva foi declarada inválida pelo Tribunal de Justiça no acórdão de 8 de abril de 2014, Digital Rights Ireland e Seitlinger e o. (C-293/12 e C-594/12, EU:C:2014:238), pelo facto de esta violar gravemente o direito ao respeito da vida privada e à proteção dos dados pessoais (v. rubrica I.1., intitulada «Conformidade do direito derivado da União com o direito à proteção dos dados pessoais» da presente ficha).

4 Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60), revogada a partir de 6 de maio de 2018 (v. nota 6).

5 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (JO L 119 de 4.5.2016) aplicável a partir de 25 de maio de 2018.

6 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

7 Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

8 Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos da Comunidade e à livre circulação desses dados e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE [COM(2017) 8 final].

I. O direito à proteção dos dados pessoais reconhecido pela Carta dos Direitos Fundamentais da União Europeia

1. Conformidade do direito derivado da União com o direito à proteção dos dados pessoais

Acórdão de 9 de novembro de 2010 (Grande Secção), Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662) [9]

Neste processo, os litígios nos processos principais opunham agricultores ao Land Hessen, a propósito da publicação no sítio Internet da Bundesanstalt für Landwirtschaft und Ernährung (Serviço Federal para a Agricultura e a Alimentação) dos dados pessoais daqueles enquanto beneficiários de fundos provenientes do Fundo Europeu Agrícola de Garantia (FEAGA) e do Fundo Europeu Agrícola de Desenvolvimento Rural (FEADER). Os referidos agricultores opuseram-se a esta publicação, alegando, em especial, que esta não era justificada por um interesse público preponderante. O Land Hessen considerava, por seu lado, que a publicação dos referidos dados resultava dos Regulamentos (CE) n.os 1290/2005 [10] e 259/2008 [11], que regem o financiamento da política agrícola comum e impõem a publicação de informações relativas a pessoas singulares beneficiárias do FEAGA e do FEADER.

Foi neste contexto que o Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha) submeteu ao Tribunal de Justiça várias questões sobre a validade de certas disposições do Regulamento (CE) n.º 1290/2005 e do Regulamento (CE) n.º 259/2008, que impõem que essas informações sejam colocadas à disposição do público, nomeadamente através de sítios Internet explorados pelos serviços nacionais.

No que respeita à adequação entre o direito à proteção dos dados pessoais reconhecido pela Carta e a transparência em matéria de fundos europeus, o Tribunal salientou que a publicação num sítio Internet de dados nominativos relativos aos beneficiários dos fundos e aos montantes recebidos por estes constitui, em razão do livre acesso por terceiros ao referido sítio, uma violação do direito dos beneficiários em causa ao respeito da sua vida privada, em geral, e à proteção dos seus dados pessoais, em particular (n.os 56-64).

Para ser justificada, essa ingerência deve ser prevista por lei, respeitar o conteúdo essencial desses direitos e, em aplicação do princípio da proporcionalidade, ser necessária e responder efetivamente a objetivos de interesse geral reconhecidos pela União, devendo as derrogações e limitações a estes direitos ocorrer na estrita medida do necessário. Neste contexto, o Tribunal considerou que embora numa sociedade democrática os contribuintes tenham o direito de ser informados sobre a utilização dos fundos públicos, não é menos verdade que o Conselho e a Comissão estavam obrigados a proceder a uma ponderação equilibrada dos interesses em causa, o que implicava, antes da adoção das disposições impugnadas, verificar se a publicação destes dados pelo Estado-Membro num sítio Internet único não ultrapassava o necessário para a realização dos objetivos legítimos prosseguidos (n.os 77, 79, 85, 86).

---

9 Este acórdão foi apresentado no Relatório Anual de 2010, p. 11.

10 Regulamento (CE) n.º 1290/2005 do Conselho, de 21 de junho de 2005, relativo ao financiamento da política agrícola comum (JO L 209 de 11.8.2005, p. 1), revogado pelo Regulamento (UE) n.º 1306/2013 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativo ao financiamento, à gestão e ao acompanhamento da Política Agrícola Comum (JO L 347 de 20.12.2013, p. 549).

11 Regulamento (CE) n.º 259/2008 da Comissão, de 18 de março de 2008, que estabelece as regras de execução do Regulamento (CE) n.º 1290/2005 do Conselho no que respeita à publicação de informação sobre os beneficiários de fundos provenientes do FEAGA e do Feader (JO L 76 de 19.3.2008, p. 28), revogado pelo Regulamento de Execução (UE) n.º 908/2014 da Comissão, de 6 de agosto de 2014, que estabelece as normas de execução do Regulamento (UE) n.º 1306/2013 do Parlamento Europeu e do Conselho no que diz respeito aos organismos pagadores e outros organismos, gestão financeira, apuramento das contas, controlos, garantias e transparência (JO L 255 de 28.8.2014, p. 59).

Assim, o Tribunal declarou inválidas certas disposições do Regulamento (CE) n.º 1290/2005, bem como o Regulamento (CE) n.º 259/2008 na totalidade, na medida em que, relativamente às pessoas singulares beneficiárias de ajudas do FEAGA e do Feader, essas disposições impõem a publicação de dados pessoais relativos a qualquer beneficiário, sem proceder a distinções de acordo com critérios pertinentes, como por exemplo os períodos durante os quais receberam essas ajudas, a sua frequência ou ainda o tipo ou a importância das mesmas (n.º 92, disp. 1). No entanto, o Tribunal não anulou os efeitos da publicação das listas dos beneficiários de tais auxílios efetuada pelas autoridades nacionais durante o período anterior à data da prolação do acórdão (n.º 94, disp. 2).

Acórdão de 17 de outubro de 2013, Schwarz (C-291/12, EU:C:2013:670)

M. Schwarz tinha solicitado a emissão de um passaporte na Stadt Bochum (Alemanha), tendo-se recusado, nessa ocasião, a autorizar a recolha das suas impressões digitais. Como a Stadt Bochum indeferiu o seu pedido, M. Scharwz interpôs recurso no Verwaltungsgericht Gelsenkirchen (tribunal administrativo de Gelsenkirchen, Alemanha) para que este município fosse obrigado a emitir o seu passaporte sem proceder à recolha das suas impressões digitais. Naquele órgão jurisdicional, M. Schwarz contestava a validade do Regulamento (CE) n.º 2252/2004 [12], que instituiu a obrigação de recolha das impressões digitais dos requerentes de passaportes, alegando, nomeadamente, que esse regulamento violava o direito à proteção dos dados pessoais e o direito ao respeito da vida privada.

Neste contexto, o Verwaltungsgericht Gelsenkirchen submeteu uma questão prejudicial ao Tribunal de Justiça, com vista a saber se o referido regulamento, na medida em que obriga o requerente de um passaporte a fornecer as suas impressões digitais e prevê a sua conservação nos passaportes, é válido, nomeadamente à luz da Carta.

O Tribunal respondeu afirmativamente, declarando que, embora a recolha e a conservação de impressões digitais pelas autoridades nacionais, regulada no artigo 1.º, n.º 2, do Regulamento (CE) n.º 2252/2004, constituam um ato lesivo dos direitos ao respeito da vida privada e à proteção dos dados pessoais, esta violação é justificada pelo objetivo de proteção dos passaportes contra a sua utilização fraudulenta.

Em primeiro lugar, a referida restrição, prevista por lei, prossegue um objetivo de interesse geral reconhecido pela União, na medida em que se destina a impedir, designadamente, a entrada ilegal de pessoas no território da União (n.os 35-38). Em seguida, a recolha e a conservação de impressões digitais são aptas a alcançar esse objetivo. Com efeito, por um lado, embora o método de verificação da identidade por meio de impressões digitais não seja totalmente fiável, reduz consideravelmente o risco de aceitação de pessoas não autorizadas. Por outro lado, a falta de concordância das impressões digitais do detentor do passaporte com os dados integrados nesse documento não significa que seja automaticamente recusada à pessoa em causa a entrada no território da União, mas tem como única consequência desencadear um controlo aprofundado destinado a comprovar definitivamente a identidade dessa pessoa (n.os 42-45).

Finalmente, quanto ao caráter necessário desse tratamento, não foi dado conhecimento ao Tribunal de medidas suficientemente eficazes, mas que lesem de forma menos gravosa os direitos reconhecidos pelos artigos 7.º e 8.º da Carta do que as medidas resultantes do método baseado nas impressões digitais (n.º 53). O artigo 1.º, n.º 2, do Regulamento (CE) n.º 2252/2004 não implica tratamentos das impressões digitais recolhidas que vão além do necessário para a realização do referido objetivo. Com efeito, o referido regulamento indica expressamente que as impressões digitais só podem ser utilizadas com o

12 Regulamento (CE) n.º 2252/2004 do Conselho, de 13 de dezembro de 2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros (JO L 385, de 29.12.2004, p. 1), na redação que lhe foi dada pelo Regulamento (CE) n.º 444/2009 do Parlamento Europeu e do Conselho, de 6 de maio de 2009 (JO L 142 de 6.6.2009, p. 1).

objetivo de verificar a autenticidade do passaporte e a identidade do seu titular. Além disso, o artigo 1.º, n.º 2, do regulamento garante uma proteção contra o risco de leitura dos dados que contenham impressões digitais por pessoas não autorizadas e só prevê a conservação das impressões digitais no próprio passaporte, o qual continua a ser propriedade exclusiva do seu titular (n.os 54-57, 60, 63).

Acórdão de 8 de abril de 2014 (Grande Secção), Digital Rights Ireland e Seitlinger e o. (processos apensos C-293/12 e C-594/12, EU:C:2014:238) [13]

O presente acórdão tem origem nos pedidos de apreciação da validade da Diretiva 2006/24/CE relativa à conservação de dados, no que respeita ao direito fundamental ao respeito da vida privada e à proteção dos dados pessoais, suscitados no âmbito de litígios nacionais em tribunais irlandeses e austríacos. No processo C-293/12, a High Court (Supremo Tribunal, Irlanda) foi chamada a conhecer de um litígio que opunha a Digital Rights às autoridades irlandesas a respeito da legalidade de medidas nacionais relativas à conservação de dados relativos a comunicações eletrónicas. No processo C-594/12, o Verfassungsgerichtshof (Tribunal Constitucional, Áustria) foi chamado a conhecer de vários recursos em matéria constitucional nos quais se pedia a anulação da disposição nacional que transpunha a Diretiva 2006/24/CE para direito austríaco.

Através dos seus pedidos de decisões prejudiciais, os órgãos jurisdicionais irlandeses e austríacos interrogaram o Tribunal de Justiça sobre a validade da Diretiva 2006/24/CE à luz dos artigos 7.º, 8.º e 11.º da Carta. Mais precisamente, esses órgãos jurisdicionais nacionais perguntaram ao Tribunal se a obrigação que, por força da referida diretiva, incumbe aos prestadores de serviços de comunicações eletrónicas acessíveis ao público ou de redes públicas de comunicações, de conservar durante um certo período dados relativos à vida privada de uma pessoa e às suas comunicações e de permitir o acesso das autoridades nacionais competentes a esses dados, constituía uma ingerência injustificada nos referidos direitos fundamentais. Os tipos de dados em causa são, designadamente, os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, entre os quais figuram, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços Internet. Estes dados permitem, designadamente, saber qual é a pessoa com quem um assinante ou um utilizador registado comunicou, e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o assinante ou o utilizador registado comunicam com certas pessoas, durante um certo período.

O Tribunal começou por declarar que, ao impor tais obrigações a estes fornecedores, as disposições da Diretiva 2006/24/CE eram constitutivas de uma ingerência particularmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais garantidos pelos artigos 7.º e 8.º da Carta. Neste contexto, o Tribunal declarou que essa ingerência podia ser justificada pela prossecução de um objetivo de interesse geral, como a luta contra a criminalidade organizada. A este respeito, o Tribunal salientou, em primeiro lugar, que a conservação dos dados imposta pela diretiva não era suscetível de violar o conteúdo essencial dos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, na medida em que não permitia tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal, e previa que os prestadores de serviços ou de redes deviam respeitar certos princípios de proteção e de segurança dos dados. Em segundo lugar, o Tribunal observou que a conservação dos dados e a sua transmissão às autoridades nacionais competentes correspondia efetivamente a um objetivo de interesse geral, concretamente a luta contra a criminalidade grave, bem como, em última análise, a segurança pública (n.os 38-44).

13 Este acórdão foi apresentado no Relatório Anual de 2014, p. 60.

No entanto, o Tribunal considerou que, ao adotar a diretiva relativa à conservação de dados, o legislador da União tinha excedido os limites impostos pelo respeito do princípio da proporcionalidade. Por conseguinte, o Tribunal declarou a diretiva inválida, tendo considerado que a ingerência de grande amplitude e de particular gravidade nos direitos fundamentais que a referida diretiva impunha não era suficientemente enquadrada de forma a garantir que se limitava ao estritamente necessário (n.º 65). A Diretiva 2006/24/CE abrangia efetivamente de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma distinção, limitação ou exceção com base no objetivo de luta contra as infrações graves (n.os 57-59). Por outro lado, a diretiva não previa nenhum critério objetivo que permitisse garantir que as autoridades nacionais competentes apenas tinham acesso aos dados e apenas podiam utilizá-los para prevenir, detetar ou agir penalmente contra infrações suscetíveis de serem consideradas suficientemente graves para justificar tal ingerência, sendo que também não previa as condições materiais e processuais desse acesso ou utilização. Por último, relativamente à duração do período de conservação dos dados, a diretiva impunha um prazo de, pelo menos, seis meses, sem proceder a qualquer distinção entre as categorias de dados em função das pessoas em causa ou da eventual utilidade dos dados relativamente ao objetivo prosseguido (n.os 63 e 64).

Por outro lado, no que respeita às exigências decorrentes do artigo 8.º, n.º 3, da Carta, o Tribunal declarou que a Diretiva 2006/24/CE não previa garantias suficientes que permitissem assegurar uma proteção eficaz dos dados contra os riscos de abuso e contra o acesso e utilização ilícitos dos dados, sendo que também não impunha que os mesmos fossem conservados no território da União.

Por conseguinte, a referida diretiva não garantia plenamente o controlo do respeito das exigências de proteção e de segurança por uma autoridade independente, apesar de tal ser expressamente exigido pela Carta (n.os 66-68).

2. Respeito do direito à proteção dos dados pessoais na aplicação do direito da União

Acórdão de 21 de dezembro de 2016 (Grande Secção), Tele2 Sverige (processos apensos C-203/15 e C-698/15, EU:C:2016:970) [14]

Na sequência do acórdão Digital Rights Ireland e Seitlinger e o., que declarou inválida a Diretiva 2006/24/CE (v. supra), o Tribunal de Justiça foi chamado a conhecer de dois processos que tinham por objeto a obrigação geral aplicável aos prestadores de serviços de comunicações eletrónicas na Suécia e no Reino Unido de conservar os dados relativos às referidas comunicações e cuja conservação estava prevista pela diretiva declarada inválida.

No dia seguinte ao da prolação do acórdão Digital Rights Ireland e Seitlinger e o., a empresa de telecomunicações Tele2 Sverige notificou à autoridade sueca de supervisão dos correios e telecomunicações a sua decisão de deixar de proceder à conservação dos dados bem como a sua intenção de apagar os dados já registados (processo C-203/15). Com efeito, o direito sueco obrigava os prestadores de serviços de comunicações eletrónicas a conservar, de forma sistemática, contínua e sem nenhuma exceção, todos os dados relativos ao tráfego e dados de localização de todos os seus assinantes e utilizadores registados relativos a todos os meios de comunicação eletrónica. No processo C-698/15, três pessoas impugnaram o regime britânico de conservação de dados que permitia ao Ministro do Interior obrigar os operadores públicos de telecomunicações a conservar todos os dados relativos a

14 Este acórdão foi apresentado no Relatório Anual de 2016, p. 62.

comunicações por um período máximo de doze meses, estando todavia excluída a conservação do conteúdo de tais comunicações.

O Kammarrätten i Stockholm (Tribunal Administrativo de Recurso de Estocolmo, Suécia) e a Court of Appeal (England & Wales) (Civil Division) (Secção Cível do Tribunal de Recurso de Inglaterra e do País de Gales, Reino Unido)] convidaram o Tribunal de Justiça a pronunciar-se sobre a interpretação do artigo 15.°, n.° 1, da Diretiva 2002/58/CE, dita «Privacidade e comunicações eletrónicas», que permite aos Estados-Membros introduzir certas exceções à obrigação, prevista nessa diretiva, de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados de tráfego.

No seu acórdão, o Tribunal começou por declarar que o artigo 15.°, n.° 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, se opõe a uma regulamentação nacional, como a sueca, que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica. Segundo o Tribunal, tal regulamentação excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige o referido artigo 15.°, n.° 1, lido à luz dos artigos acima referidos da Carta (n.os 99-105, 107, 112, disp. 1).

Esta mesma disposição, lida à luz desses mesmos artigos da Carta, também se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar esse acesso, no âmbito da luta contra a criminalidade, apenas à luta contra a criminalidade grave, sem submeter o referido acesso a fiscalização prévia por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados no território da União (n.os 118-122, 125, disp. 2).

O Tribunal considerou em contrapartida que o artigo 15.°, n.° 1, da Diretiva 2002/58/CE não se opõe a uma regulamentação que permite, a título preventivo, com vista à luta contra a criminalidade grave, a conservação seletiva de dados desta natureza, desde que a sua conservação seja limitada ao estritamente necessário no que se refere às categorias de dados abrangidas, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada. Para cumprir esses requisitos, esta regulamentação nacional deve, em primeiro lugar, prever normas claras e precisas que permitam proteger eficazmente os dados contra os riscos de abuso. Deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida de conservação dos dados, a título preventivo, garantindo assim que essa medida se limita ao estritamente necessário. Em segundo lugar, no que se refere às condições materiais a que deve obedecer a regulamentação nacional, de modo a assegurar que se limita ao estritamente necessário, a conservação dos dados deve sempre responder a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido. Em especial, tais condições devem revelar-se, na prática, suscetíveis de limitar efetivamente o alcance da medida e, consequentemente, o público afetado. No que se refere a esta delimitação, a regulamentação nacional deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir, seja de que maneira for, para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública (n.os 108-111).

II. O tratamento dos dados pessoais na aceção da Diretiva n.° 95/46/CE

1. Tratamento de dados pessoais excluídos do âmbito de aplicação da Diretiva 95/46/CE

Acórdão de 30 de maio de 2006 (Grande Secção), Parlamento/Conselho (C-317/04 e C-318/04, EU:C:2006:346)

Após os ataques terroristas de 11 de setembro de 2001, os Estados Unidos adotaram uma legislação que dispunha que as transportadoras aéreas que assegurassem ligações com destino ao território dos Estados Unidos ou partida desse território, ou que por ele passassem, eram obrigadas a fornecer às autoridades aduaneiras americanas um acesso eletrónico aos dados contidos nos seus sistemas automáticos de reserva e de controlo das partidas, denominados «Passenger Name Records» (a seguir «PNR»).

Considerando que estas disposições podiam ser contrárias à legislação europeia e às legislações dos Estados-Membros em matéria de proteção dos dados, a Comissão iniciou negociações com as autoridades americanas. Na sequência dessas negociações, em 14 de maio de 2004, a Comissão adotou a Decisão 2004/535/CE [15], que declarava que o Serviço das Alfândegas e Proteção das Fronteiras dos Estados Unidos (United States Bureau of Customs and Border Protection, a seguir «CBP») assegurava um nível adequado de proteção dos dados dos PNR transferidos a partir da Comunidade (a seguir «decisão de adequação»). Em seguida, em 17 de maio de 2004, o Conselho adotou a Decisão 2004/496/CE [16] que aprovava a celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência para o CBP dos dados PNR por parte das transportadoras aéreas com sede no território dos Estados-Membros da Comunidade.

O Parlamento Europeu pediu ao Tribunal de Justiça que anulasse as duas decisões acima referidas, alegando, nomeadamente, que a decisão de adequação tinha sido adotada ultra vires, que o artigo 95.° CE (atual artigo 114.° TFUE) não era uma base jurídica adequada para a decisão de aprovação da celebração do Acordo e que em ambos os casos havia uma violação dos direitos fundamentais.

No que respeita à decisão de adequação, o Tribunal começou por examinar se a Comissão podia validamente adotar a sua decisão com fundamento na Diretiva 95/46/CE. Neste contexto, constatou que decorria da decisão de adequação que a transferência dos dados PNR para o CBP constituía um tratamento que tinha por objeto a segurança pública e as atividades do Estado no domínio do direito penal. Segundo o Tribunal, embora os dados PNR fossem inicialmente recolhidos pelas companhias aéreas no âmbito de uma atividade abrangida pelo direito da União, a saber, a venda de um bilhete de avião que confere o direito a uma prestação de serviços, o tratamento dos dados que era tomado em conta na decisão de adequação era de natureza completamente diferente. Com efeito, esta decisão não visava um tratamento de dados necessário para a realização de uma prestação de serviços, mas um tratamento de dados considerado necessário para salvaguarda da segurança pública e para fins repressivos (n.os 56, 57).

15 Decisão 2004/535/CE da Comissão, de 14 de maio de 2004, sobre o nível de proteção adequado dos dados pessoais contidos nos Passenger Name Record transferidos para o Bureau of Customs and Border Protection dos Estados Unidos (JO L 235 de 6.7.2004, p. 11).

16 Decisão 2004/496/CE do Conselho, de 17 de maio de 2004, relativa à celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência de dados contidos nos registos de identificação dos passageiros (PNR) por parte das transportadoras aéreas para o Serviço das Alfândegas e Proteção das Fronteiras do Departamento de Segurança Interna dos Estados Unidos (JO L 183 de 20.5.2004, p. 83, e retificativo JO L 255 de 30.9.2005, p. 168).

A este respeito, o Tribunal considerou que o facto de os dados PNR terem sido recolhidos por operadores privados para fins comerciais e de serem estes últimos a organizar a sua transferência para um Estado terceiro não se opunha a que essa transferência fosse considerada um tratamento de dados excluído do âmbito de aplicação da diretiva. Com efeito, essa transferência integrava-se num quadro instituído pelos poderes públicos e que visava a segurança pública. Por conseguinte, o Tribunal concluiu que a decisão de adequação não era abrangida pelo âmbito de aplicação da diretiva, uma vez que dizia respeito a um tratamento de dados pessoais que estava excluído da mesma. Por conseguinte, o Tribunal anulou a decisão de adequação (n.os 58, 59).

No que se refere à decisão do Conselho, o Tribunal declarou que o artigo 95.° CE, lido em conjugação com o artigo 25.° da Diretiva 95/46/CE, não é suscetível de servir de base à competência da Comunidade para celebrar o acordo em questão com os Estados Unidos. Com efeito, este acordo tinha em vista a mesma transferência de dados que a decisão de adequação e, portanto, tratamentos de dados que estavam excluídos do âmbito de aplicação da diretiva. Por conseguinte, o Tribunal anulou a decisão do Conselho que aprovou a celebração do acordo (n.os 67-69).

Acórdão de 11 de dezembro de 2014, Ryneš (C-212/13, EU:C:2014:2428)

Em resposta a agressões repetidas, F. Ryneš instalou em sua casa uma câmara de vigilância. Na sequência de um novo ataque à sua casa, os registos da referida câmara permitiram identificar dois suspeitos, contra os quais foram instaurados processos penais. Tendo a legalidade do tratamento dos dados registados pela câmara de vigilância sido contestada por um dos suspeitos perante o Instituto Checo para a proteção dos dados pessoais, este tinha constatado que F. Ryneš tinha violado as regras em matéria de proteção dos dados pessoais e aplicado uma coima a este último.

Chamado a conhecer de um recurso interposto por F. Ryneš contra uma decisão do Městský soud v Praze (Tribunal da Comarca de Praga, República Checa) que tinha confirmado a decisão do Instituto, o Nejvyšší správní soud (Supremo Tribunal Administrativo, República Checa) perguntou ao Tribunal de Justiça se a gravação vídeo efetuada por F. Ryneš para proteger a sua vida, a sua saúde e os seus bens constituía um tratamento de dados não abrangido pela Diretiva 95/46/CE pelo facto de o registo ter sido efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, na aceção do artigo 3.°, n.° 2, segundo travessão, da referida diretiva.

O Tribunal declarou que a exploração de um sistema de câmara que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição (n.° 35 e disp.).

A este respeito, o Tribunal recordou que a proteção do direito fundamental ao respeito da vida privada, garantido pelo artigo 7.° da Carta, exige que as derrogações à proteção dos dados pessoais e as respetivas limitações ocorram na estrita medida do necessário. Na medida em que as disposições da Diretiva 95/46/CE, que regulam o tratamento de dados pessoais suscetíveis de pôr em causa as liberdades fundamentais, em especial o direito à vida privada, devem, necessariamente, ser interpretadas à luz dos direitos fundamentais que estão consagrados na referida Carta, a derrogação prevista no artigo 3.°, n.° 2, segundo travessão, desta diretiva deve ser objeto de interpretação estrita (n.os 27-29). Além disso, a própria letra desta disposição exclui do âmbito de aplicação da Diretiva 95/46/CE o tratamento de dados efetuado no exercício de atividades «exclusivamente» pessoais ou domésticas. Ora, na medida em que uma videovigilância se estende, ainda que parcialmente, ao espaço público e, por esse motivo, se dirige para fora da esfera privada da pessoa que procede ao tratamento de

dados por esse meio, não pode ser considerada uma atividade exclusivamente «pessoal ou doméstica», na aceção da referida disposição (n.os 30, 31, 33).

2. Conceito de «dados pessoais»

Acórdão de 19 de outubro de 2016, Breyer (C-582/14, EU:C:2016:779) [17]

P. Breyer tinha intentado uma ação nos tribunais cíveis alemães para que a República Federal da Alemanha fosse proibida de conservar ou mandar conservar por terceiros dados informáticos que eram transmitidos após o termo de cada consulta dos sítios Internet dos serviços federais alemães. Com efeito, a fim de se proteger de ataques e de permitir ações penais contra «piratas», o prestador de serviços de meios de comunicação em linha dos serviços federais alemães gravava dados constituídos por um endereço IP «dinâmico» — um endereço IP que muda por ocasião de cada nova ligação a Internet – bem como a data e a hora da sessão de consulta do sítio. Contrariamente aos endereços IP estáticos, os endereços IP dinâmicos não permitem fazer a ligação a priori, através de ficheiros acessíveis ao público, entre um determinado computador e a ligação física à rede utilizada pelo fornecedor de acesso à Internet. Os dados registados, por si só, não ofereciam ao fornecedor de serviços de comunicação social em linha a possibilidade de identificar o utilizador. Em contrapartida, por sua vez, o fornecedor de acesso à Internet dispunha de informações suplementares que caso fossem combinadas com esse endereço IP permitiam identificar o referido utilizador.

Neste contexto, o Bundesgerichtshof (Tribunal Federal de Justiça, Alemanha), chamado a pronunciar-se em sede de um recurso de «Revision», interrogou o Tribunal de Justiça sobre a questão de saber se um endereço IP que é registado por um prestador de serviços de meios de comunicação em linha quando acede ao seu sítio Internet constitui um dado pessoal.

O Tribunal começou por observar que, para que um dado possa ser qualificado de «dado pessoal», na aceção do artigo 2.°, alínea a), da Diretiva 95/46/CE, não é necessário que todas as informações que permitem identificar a pessoa em causa estejam na posse de uma única pessoa. O facto de as informações suplementares necessárias para identificar o utilizador de um sítio Internet não serem detidas pelo prestador de serviços de meios de comunicação em linha, mas pelo fornecedor de acesso à Internet desse utilizador, não parece, assim, suscetível de excluir que os endereços IP dinâmicos registados pelo prestador de serviços de meios de comunicação em linha constituam, para este, dados pessoais na aceção do artigo 2.°, alínea a), da Diretiva 95/46/CE (n.os 43, 44).

Por conseguinte, o Tribunal constatou que um IP dinâmico, registado por um prestador de serviços de meios de comunicação em linha quando alguém consulta um sítio Internet que esse prestador disponibiliza ao público, constitui, relativamente a esse prestador, um dado pessoal na aceção do artigo 2.°, alínea a), da Diretiva 95/46/CE, quando este disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares de que o fornecedor de acesso à Internet dessa pessoa dispõe (n.° 49, disp. 1).

Acórdão de 20 de dezembro de 2017, Nowak (C-434/16, ECLI:EU:C:2017:582)

M. Nowak, um contabilista estagiário, reprovou no exame organizado pela Câmara irlandesa dos técnicos oficiais de contas. M. Nowak tinha apresentado um pedido de acesso a todos os dados pessoais que lhe diziam respeito detidos pela Câmara dos técnicos oficiais de contas, ao abrigo do artigo 4.° da lei de

17 Este acórdão foi apresentado no Relatório Anual de 2016, p. 61.

proteção de dados. Esta última tinha comunicado a P. Nowak alguns documentos, mas recusou-se a entregar-lhe a cópia do seu exame pelo facto de a mesma não conter dados pessoais relativos ao requerente, na aceção da lei relativa à proteção dos dados.

Na medida em que, pelos mesmos motivos, o Comissário para a proteção dos dados também não deferiu o seu pedido de acesso, M. Nowak intentou uma ação nos órgãos jurisdicionais nacionais. A Supreme Court (Supremo Tribunal, Irlanda), chamada a conhecer de um recurso interposto por M. Nowak, submeteu ao Tribunal de Justiça a questão de saber se o artigo 2.°, alínea a), da Diretiva 95/46/CE deve ser interpretado no sentido de que, em condições como as que estão em causa no processo principal, as respostas escritas dadas por um candidato durante um exame profissional e as eventuais anotações do examinador com elas relacionadas constituem dados pessoais na aceção dessa disposição.

Em primeiro lugar, o Tribunal considerou que, para que um dado possa ser qualificado de «dado pessoal», na aceção do artigo 2.°, alínea a), da Diretiva 95/46/CE, não é necessário que todas as informações que permitem identificar a pessoa em causa estejam na posse de uma única pessoa. Por outro lado, na hipótese de o examinador não conhecer a identidade do candidato aquando da notação das respostas dadas por este num exame, a entidade que organiza o exame, no caso em apreço, a Câmara dos técnicos oficiais de contas, dispõe, em contrapartida, das informações necessárias que lhe permitem identificar o candidato sem qualquer dificuldade ou dúvida a partir do seu número de identificação inscrito na folha de respostas do exame ou na capa da mesma, e, assim, identificar as suas respostas.

Em segundo lugar, o Tribunal concluiu que as respostas escritas fornecidas por um candidato num exame profissional constituem informações relacionadas com a sua pessoa. Com efeito, o conteúdo dessas respostas reflete o nível de conhecimentos e de competência do candidato num dado domínio, bem como, sendo caso disso, o seu processo de reflexão, o seu julgamento e o seu espírito crítico. Além disso, a recolha das referidas respostas tem como finalidade avaliar as capacidades profissionais do candidato e a sua aptidão para exercer a profissão em causa. Acresce que a utilização dessas informações, que se traduz, designadamente, pela aprovação ou reprovação do candidato no exame em causa, é suscetível de ter um efeito sobre os seus direitos e interesses, na medida em que pode determinar ou influenciar, por exemplo, as possibilidades de esse candidato aceder à profissão ou ao emprego pretendidos. A conclusão de que as respostas escritas dadas por um candidato num exame profissional constituem informações que dizem respeito a esse candidato devido ao seu conteúdo, à sua finalidade e ao seu efeito é válida igualmente quando se trate de um exame com consulta.

Em terceiro lugar, no que respeita às anotações do examinador relativas às respostas do candidato, o Tribunal considerou que estas constituem, juntamente com as respostas do candidato no exame, informações sobre esse candidato, uma vez que refletem a opinião ou a apreciação do examinador quanto à prestação individual do candidato no exame e, designadamente, quanto aos seus conhecimentos e às suas competências no domínio em causa. Além disso, as referidas anotações têm precisamente como finalidade documentar a avaliação da prestação do candidato feita pelo examinador e são suscetíveis de ter efeitos para este último.

Em quarto lugar, o Tribunal considerou que as respostas escritas dadas por um candidato num exame profissional e as eventuais anotações do examinador com elas relacionadas podem estar sujeitas a uma verificação, designadamente, da respetiva exatidão e da necessidade da sua conservação, na aceção do artigo 6.°, n.° 1, alíneas d) e e), da Diretiva 95/46, e podem ser objeto de uma retificação ou de um apagamento, ao abrigo do seu artigo 12.°, alínea b). O facto de conferir ao candidato um direito de acesso a essas respostas e a essas anotações, nos termos do artigo 12.°, alínea a), desta diretiva, serve o objetivo desta última, que consiste em garantir a proteção do direito à vida privada desse candidato relativamente ao tratamento dos dados que lhe dizem respeito e tal independentemente da questão de saber se o referido candidato dispõe ou não desse direito de acesso, igualmente ao abrigo da legislação nacional aplicável ao procedimento de exame. No entanto, o Tribunal sublinhou que os direitos de acesso

e de retificação, ao abrigo do artigo 12.°, alíneas a) e b), da Diretiva 95/46/CE, não são extensivos às questões do exame, que não constituem, enquanto tais, dados pessoais do candidato.

Tendo em conta estes elementos, o Tribunal concluiu que, em condições como as que estavam em causa no processo principal, as respostas escritas fornecidas por um candidato num exame profissional e as anotações do examinador relativas a essas respostas constituem dados pessoais, na aceção do artigo 2.°, alínea a), da Diretiva 95/46/CE.

3. Conceito de «tratamento de dados pessoais»

Acórdão de 6 de novembro de 2003 (Assembleia Plenária), Lindqvist (C-101/01, EU:C:2003:596)

B. Lindqvist, trabalhadora voluntária numa paróquia da Igreja Protestante na Suécia, criou páginas Internet com o seu computador pessoal nas quais publicou dados pessoais sobre várias pessoas que, como ela, trabalhavam como voluntárias na referida paróquia. B. Lindqvist foi condenada no pagamento de uma coima por ter utilizado dados pessoais no contexto de um tratamento automatizado sem ter previamente procedido à declaração escrita junto da Datainspektion sueca (organismo público para a proteção dos dados transmitidos por via informática), por ter transferido esses dados sem autorização para países terceiros e por ter tratado dados pessoais sensíveis.

No âmbito do recurso interposto por B. Lindqvist desta decisão no Göta hovrätt (tribunal de recurso, Suécia), este último interrogou o Tribunal de Justiça a título prejudicial com vista a saber, em particular, se B. Lindqvist tinha procedido a um «tratamento de dados pessoais por meios total ou parcialmente automatizados» na aceção da Diretiva 95/46/CE.

O Tribunal declarou que a operação que consiste na referência, numa página da Internet, a várias pessoas e à sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui um «tratamento de dados pessoais por meios total ou parcialmente automatizados», na aceção desta diretiva (n.° 27, disp. 1). Com efeito, tal tratamento de dados pessoais, efetuado para o exercício de atividades benévolas ou religiosas, não é abrangido por nenhuma das exceções ao âmbito de aplicação da diretiva, na medida em que não se integra nem na categoria de atividades que têm por objeto a segurança pública nem na categoria de atividades exclusivamente pessoais ou domésticas que estão fora do âmbito de aplicação da diretiva (n.^{os} 38, 43-48, disp. 2).

Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317)

Em 2010, um cidadão espanhol apresentou à Agencia Española de Protección de Datos (Agência Espanhola de Proteção de Dados, a seguir «AEPD») uma reclamação contra a La Vanguardia Ediciones SL, editora de um jornal de grande tiragem em Espanha, bem como contra a Google Spain e a Google. Essa pessoa alegava que, quando um internauta inseria o seu nome no motor de busca do grupo Google, a lista de resultados tinha ligações a duas páginas do jornal La Vanguardia, datados de 1998, em que se anunciava uma venda de imóveis em hasta pública na sequência de um arresto com vista à recuperação das suas dívidas. Com esta reclamação, M. Costeja González pedia, por um lado, que se ordenasse ao La Vanguardia que suprimisse ou alterasse as referidas páginas ou que se utilizassem certas ferramentas disponibilizadas pelos motores de busca para proteger esses dados. Por outro lado, pedia que a Google Spain ou z Google Inc. fossem intimadas a suprimir ou a ocultar os seus dados pessoais, para que os mesmos deixassem de ser exibidos nos resultados de pesquisa e de figurar nas ligações do La Vanguardia.

A AEPD tinha indeferido a reclamação contra o La Vanguardia, considerando que as informações em causa tinham sido legalmente publicadas pelo editor, mas, em contrapartida, deferiu-a relativamente à Google Spain e à Google, tendo requerido a estas duas sociedades que adotassem as medidas necessárias para retirar os dados do seu índice e para impossibilitar o acesso às mesmas no futuro. Tendo as referidas sociedades interposto recurso perante a Audiencia Nacional (Audiência Nacional, Espanha), a fim de obter a anulação da decisão da AEPD, o órgão jurisdicional espanhol apresentou uma série de questões ao Tribunal de Justiça.

Assim, o Tribunal de Justiça teve a oportunidade de precisar o conceito de «tratamento de dados pessoais» na Internet em conformidade com a Diretiva 95/46/CE.

O Tribunal declarou assim que a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por uma determinada ordem de preferência deve ser qualificada de tratamento de dados pessoais quando essas informações contenham dados pessoais (disp. 1). O Tribunal recordou, além disso, que as operações visadas pela diretiva devem ser qualificadas de tratamento, incluindo quando são exclusivamente relativas a informações já publicadas nos meios de comunicação social. Uma derrogação geral à aplicação da diretiva neste caso teria por efeito esvaziá-la amplamente do seu sentido (n.os 29, 30).

4. Requisitos de licitude de um tratamento de dados pessoais ao abrigo do artigo 7.° da Diretiva 95/46/CE

Acórdão de 16 de dezembro de 2008 (Grande Secção), Huber (C-524/06, EU:C:2008:724) [18]

O Serviço Federal das Migrações e Refugiados (Bundesamt für Migration und Flüchtlinge, Alemanha), assegurava a gestão de um registo central dos estrangeiros que reunia certos dados pessoais relativos aos estrangeiros que residiam no território alemão por um período superior a três meses. O registo era utilizado para fins estatísticos pelos serviços de segurança e de polícia, assim como pelas autoridades judiciárias, no exercício de competências no domínio do processo penal e em investigações de atos criminosos ou de atos que pusessem em perigo a ordem pública.

H. Huber, nacional austríaco, instalou-se na Alemanha em 1996 para aí exercer a profissão de agente de seguros por conta própria. Por se considerar discriminado devido ao tratamento de que eram objeto os seus dados constantes do registo em causa, uma vez que essa base de dados não existia para os nacionais alemães, H. Huber requereu a supressão dos dados em causa.

Neste contexto, o Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tribunal Administrativo Superior do Land da Renânia do Norte-Vestefália, Alemanha), chamado a conhecer do litígio, interrogou o Tribunal de Justiça sobre a compatibilidade com o direito da União do tratamento de dados pessoais a que se tinha procedido no registo em causa.

O Tribunal recordou, em primeiro lugar, que o direito de residência de um cidadão da União no território de um Estado-Membro do qual não é nacional não é incondicional, podendo ser sujeito a limitações. Por isso, a utilização de um registo com a finalidade de dar apoio às autoridades encarregues da aplicação da legislação sobre o direito de residência é, em princípio, legítima e, dada a sua natureza, compatível com a proibição de discriminação em razão da nacionalidade constante do artigo 12.°, primeiro parágrafo, CE (atual artigo 18.°, primeiro parágrafo, TFUE). Todavia, tal registo não pode conter informações diferentes

18 Este acórdão foi apresentado no Relatório Anual de 2008, p. 45.

das necessárias para essa finalidade na aceção da diretiva sobre a proteção de dados pessoais (n.os 54, 58, 59).

No que diz respeito ao conceito de necessidade do tratamento na aceção do artigo 7.°, alínea e), da Diretiva 95/46/CE, o Tribunal começou por recordar que se tratava de um conceito autónomo do direito da União que deve receber uma interpretação suscetível de cumprir plenamente o objetivo da Diretiva 95/46/CE, definido no seu artigo 1.°, n.° 1. Em seguida, o Tribunal constatou que um sistema de tratamento de dados pessoais só é conforme ao direito da União se contiver unicamente os dados necessários à aplicação dessa legislação pelas referidas autoridades e o seu caráter centralizado permitir uma aplicação mais eficaz dessa legislação no que respeita ao direito de residência dos cidadãos da União Europeia que não são nacionais desse Estado-Membro.

Em todo o caso, não se podem considerar necessários, na aceção do artigo 7.°, alínea e), da Diretiva 95/46/CE, a conservação e tratamento de dados pessoais nominativos no âmbito de um registo como o registo central dos estrangeiros para fins estatísticos (n.os 52, 66, 68).

Por outro lado, no que respeita à questão da utilização das informações contidas no registo para efeitos de luta contra a criminalidade, o Tribunal observou, nomeadamente, que este objetivo visa a repressão dos crimes e dos delitos cometidos, independentemente da nacionalidade dos seus autores. Por esta razão, para um Estado-Membro, a situação dos seus nacionais não pode ser diferente da dos cidadãos da União que não são nacionais desse Estado-Membro e residem no seu território, face ao objetivo de combate à criminalidade. Por conseguinte, a diferença de tratamento entre esses nacionais e esses cidadãos da União Europeia induzida pelo tratamento sistemático dos dados pessoais respeitantes unicamente aos cidadãos da União Europeia que não são nacionais do Estado-Membro em causa com o objetivo de combater a criminalidade constitui uma discriminação proibida pelo artigo 12.°, primeiro parágrafo, CE (n.os 78-80).

Acórdão de 24 de novembro de 2011, ASNEF e FECEMD (C-468/10 e C-469/10, EU:C:2011:777)

A Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), por um lado, e a Federación de Comercio Eletrónico y Marketing Direto (FECEMD), por outro, interpuseram no Tribunal Supremo (Espanha) um recurso contencioso de anulação de vários artigos do Real Decreto 1720/2007 que aplicava a Lei Orgânica 15/1999, que tinha transposto a Diretiva 95/46/CE.

Em especial, a ASNEF e a FECEMD consideravam que, para permitir o tratamento de dados pessoais na falta de consentimento da pessoa em causa, o direito espanhol acrescentava um requisito que não existe na Diretiva 95/46/CE, exigindo que os referidos dados constem de «fontes acessíveis ao público», tal como enumeradas no artigo 3.°, alínea j), da Lei Orgânica 15/1999. A este respeito, alegaram que essa lei e o Real Decreto 1720/2007 restringiam o alcance do artigo 7.°, alínea f), da Diretiva 95/46/CE, que sujeita o tratamento de dados de caráter pessoal, na falta do consentimento da pessoa em causa, a uma requisito exclusivamente relativo ao interesse legítimo prosseguido pelo responsável pelo tratamento ou pelo terceiro ou terceiros a quem os dados sejam comunicados.

A este respeito, o Tribunal salientou, antes de mais, que o artigo 7.° da Diretiva 95/46/CE prevê uma lista exaustiva e taxativa dos casos em que um tratamento de dados pessoais pode ser considerado lícito na falta de consentimento da pessoa em causa. Por conseguinte, os Estados-Membros também não podem introduzir, ao abrigo do artigo 5.° da referida diretiva, outros princípios relativos à legitimação de tratamentos de dados pessoais além dos enunciados no artigo 7.° nem alterar, através de exigências suplementares, o alcance dos princípios previstos no referido artigo 7.° Com efeito, o artigo 5.° só autoriza os Estados-Membros a precisar, nos limites do capítulo II da referida diretiva e, logo, do artigo 7.° da mesma, as condições em que os tratamentos de dados pessoais são lícitos (n.os 30, 32, 33).

Em particular, para efetuarem a necessária ponderação dos direitos e interesses opostos em causa, prevista no artigo 7.°, alínea f), da referida diretiva, os Estados-Membros podem prever princípios orientadores. Os Estados-Membros podem igualmente tomar em consideração o facto de a gravidade da violação dos direitos fundamentais da pessoa em causa no tratamento poder variar em função da questão de saber se os referidos dados em causa já constam, ou não, de fontes acessíveis ao público (n.os 44 e 46).

Contudo, o Tribunal considerou que já não está em causa uma especificação na aceção do artigo 5.° da Diretiva 95/46/CE se uma regulamentação nacional exclui a possibilidade de algumas categorias de dados pessoais serem tratadas prescrevendo, para essas categorias, de forma definitiva, o resultado da ponderação dos direitos e interesses opostos, sem permitir um resultado diferente devido a circunstâncias particulares de um caso concreto. Por conseguinte, o Tribunal concluiu que o artigo 7.°, alínea f), da Diretiva 95/46/CE se opõe a que um Estado-Membro exclua de forma categórica e generalizada a possibilidade de algumas categorias de dados pessoais serem tratadas sem permitir que num caso específico se proceda a uma ponderação dos direitos e interesses opostos em causa (n.os 47, 48).

Acórdão de 19 de outubro de 2016, Breyer (C-582/14, EU:C:2016:779)

Neste acórdão (v. igualmente a rubrica II.2., intitulada «Conceito de «dados pessoais») o Tribunal de Justiça também se pronunciou sobre a questão de saber se o artigo 7.°, alínea f), da Diretiva 95/46/CE se opõe a uma disposição de direito nacional nos termos da qual o prestador de serviços de meios de comunicação em linha apenas pode recolher e utilizar dados pessoais de um utilizador sem o seu consentimento, na medida em que tal seja necessário para permitir e faturar a utilização concreta do meio de comunicação em linha por parte desse utilizador, e nos termos da qual a finalidade de garantir o funcionamento geral do meio de comunicação em linha não pode justificar a sua utilização após o termo da sessão de consulta em curso.

O Tribunal declarou que o artigo 7.°, alínea f), da Diretiva 95/46/CE se opõe à regulamentação em causa. Com efeito, ao abrigo desta disposição, o tratamento de dados pessoais, na aceção da mesma, é considerado lícito se o tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa. Ora, no caso em apreço, a regulamentação alemã excluía de forma categórica e generalizada a possibilidade de algumas categorias de dados pessoais serem tratadas, sem permitir uma ponderação dos direitos e interesses opostos em causa num caso específico. Ao fazê-lo, reduziu ilicitamente o âmbito deste princípio previsto no artigo 7.°, alínea f), da Diretiva 95/46/CE, impedindo que o objetivo de garantir a capacidade geral de funcionamento dos sítios Internet do meio de comunicação em linha pudesse ser objeto de ponderação com o interesse ou os direitos e liberdades fundamentais dos utilizadores (n.os 62-64, disp. 2).

Acórdão de 4 de maio de 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Este processo inscreve-se no âmbito de um litígio que opunha a polícia nacional letã à Rīgas satiksme, sociedade de tróleis da cidade de Riga, relativo a um pedido de comunicação dos dados de identificação do autor de um acidente. No caso em apreço, num acidente de circulação rodoviária, um taxista tinha estacionado o seu veículo junto ao passeio. No momento em que o trólei da Rīgas satiksme circulava junto a este táxi, o passageiro que ocupava o banco traseiro do referido táxi abriu a porta, que bateu na carroçaria do trólei, danificando-a. Para instaurar uma ação cível, a Rīgas satiksme pediu, nomeadamente, à polícia nacional a comunicação dos dados de identificação do autor do acidente. A polícia tinha recusado comunicar o número do documento de identificação e o endereço do passageiro bem como os documentos relativos às declarações prestadas pelas pessoas envolvidas no acidente pelo

facto de os documentos relativos a um processo administrativo sancionatório só poderem ser comunicados às partes nesse processo, e, no que respeita ao número de identificação e ao endereço, a Lei de proteção dos dados das pessoas singulares proibir a divulgação de tais informações sobre particulares.

Nestas condições, o Augstākās tiesas Administratīvo lietu departaments (Supremo Tribunal, Secção de Contencioso Administrativo, Letónia) submeteu ao Tribunal de Justiça a questão de saber se o artigo 7.º, alínea f), da Diretiva 95/46/CE, impõe a obrigação de comunicar dados pessoais a um terceiro para permitir que este último instaure uma ação de indemnização num tribunal cível por um dano causado pela pessoa interessada na proteção desses dados e se o facto de essa pessoa ser menor pode ser relevante para a interpretação desta disposição.

O Tribunal declarou que o artigo 7.º, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que não impõe a obrigação de comunicar dados pessoais a um terceiro a fim de lhe permitir instaurar uma ação de indemnização num tribunal cível por um dano causado pela pessoa interessada na proteção desses dados. Todavia, a referida disposição não se opõe a essa comunicação no caso de a mesma ser efetuada com base no direito nacional, respeitando os requisitos previstos nesta disposição (n.os 27, 34 e disp.).

Neste contexto, o Tribunal observou que, sem prejuízo das verificações a efetuar a este respeito pelo juiz nacional, não se afigura justificado, em condições como as que estão em causa no processo principal, recusar a uma parte lesada a comunicação dos dados pessoais necessária à propositura de uma ação de indemnização contra o autor do dano ou, sendo caso disso, contra as pessoas que exerçam o poder parental, pelo facto de esse autor ser menor (n.º 33).

Acórdão de 27 de setembro de 2017, Puškár (C-73/16, EU:C:2017:725)

No processo principal, P. Puškár tinha interposto um recurso no Najvyšší súd Slovenskej republiky (Supremo Tribunal da República Eslovaca) requerendo que o Finančné riaditel'stvo (Direção de Finanças), todas as autoridades fiscais sob o seu controlo e o Kriminálny úrad finančnej správy (Serviço de Luta contra a Criminalidade Financeira) fossem intimados a não inscrever o seu nome na lista de pessoas consideradas pela Direção de Finanças como testas de ferro, elaborada no âmbito da cobrança de impostos, e cuja atualização era assegurada pela Direção de Finanças, bem como pelo departamento de luta contra a criminalidade financeira (a seguir «lista controvertida»). Além disso, tinha pedido que fosse suprimida qualquer referência a seu respeito dessas listas e do sistema informático da administração financeira.

Nestas condições, o Najvyšší súd submeteu ao Tribunal de Justiça a questão de saber, nomeadamente, se o direito ao respeito da vida privada e familiar e das comunicações, consagrado no artigo 7.º, e o direito à proteção dos dados pessoais, consagrado no artigo 8.º da Carta, podem ser interpretados no sentido de que um Estado-Membro não pode, sem o consentimento do interessado, elaborar listas de dados pessoais para efeitos da cobrança de impostos, na medida em que a obtenção de dados pessoais pelas autoridades públicas para combater a fraude fiscal poderia, em si mesma, constituir um risco.

O Tribunal concluiu que o artigo 7.º, alínea e), da Diretiva 95/46 não se opõe a um tratamento de dados pessoais pelas autoridades de um Estado-Membro para efeitos da cobrança de impostos e de luta contra a fraude fiscal, como o que consistiu na criação da lista controvertida no processo principal, sem o consentimento das pessoas em causa, desde que, por um lado, essas autoridades tenham sido investidas pela legislação nacional de missões de interesse público, na aceção desta disposição, de que a criação dessa lista e a inscrição do nome das pessoas em causa sejam efetivamente adequadas e necessárias para alcançar os objetivos prosseguidos e de que haja indícios suficientes para presumir que a inscrição

das pessoas em causa na lista é justificada e, por outro, de que estejam cumpridos todos os requisitos de licitude deste tratamento de dados pessoais impostos pela Diretiva 95/46 (n.º 117, disp. 3).

A este respeito, o Tribunal declarou que incumbe ao órgão jurisdicional de reenvio verificar se a criação da lista controvertida é necessária para a execução das missões de interesse público em causa no processo principal, atendendo, designadamente, à finalidade exata da criação da lista controvertida, aos efeitos jurídicos a que estão sujeitas as pessoas que nela figuram e ao caráter público ou não dessa lista. Além disso, à luz do princípio da proporcionalidade, cabe ao órgão jurisdicional nacional verificar se a criação da lista controvertida e a inscrição na mesma do nome das pessoas em causa são adequadas para alcançar os objetivos prosseguidos e se não existem outras medidas menos restritivas para alcançar os referidos objetivos (n.os 111, 112, 113).

Além disso, o Tribunal constatou que o facto de uma pessoa estar inscrita na lista controvertida pode pôr em causa alguns dos seus direitos. Com efeito, a inscrição nessa lista pode prejudicar a sua reputação e afetar as suas relações com as autoridades fiscais. De igual modo, esta inscrição pode afetar a presunção de inocência dessa pessoa, consagrada no artigo 48.º, n.º 1, da Carta, bem como a liberdade de empresa, prevista no artigo 16.º da Carta, das pessoas coletivas associadas às pessoas singulares inscritas na lista controvertida. Por conseguinte, tal afetação só pode ser adequada se houver indícios suficientes para suspeitar que a pessoa em causa ocupa de forma fictícia um cargo de direção nas pessoas coletivas que lhe estão associadas e que, desse modo, prejudica a cobrança dos impostos e a luta contra a fraude fiscal (n.º 114).

Por outro lado, o Tribunal considerou que se existirem motivos para restringir, ao abrigo do artigo 13.º da Diretiva 95/46/CE, certos direitos previstos nos artigos 6.º e 10.º a 12.º desta diretiva, como o direito à informação da pessoa em causa, essa restrição deve ser necessária à proteção de um interesse mencionado no n.º 1 do referido artigo 13.º, como, designadamente, um interesse económico ou financeiro importante no domínio fiscal, e basear-se em medidas legislativas (n.º 116).

III. Transferência de dados pessoais para países terceiros

Acórdão de 6 de novembro de 2003 (Assembleia Plenária), Lindqvist (C-101/01, EU:C:2003:596) [19]

Neste processo (v. igualmente rubrica II.3., intitulada «Conceito de 'tratamento de dados pessoais'»), o órgão jurisdicional de reenvio pretendia, em particular, saber se B. Lindqvist tinha procedido a uma transferência de dados para um país terceiro na aceção da diretiva.

O Tribunal de Justiça declarou que não existe uma «transferência para um país terceiro de dados pessoais» na aceção do artigo 25.º da Diretiva 95/46/CE, quando uma pessoa que se encontra num Estado-Membro insere dados pessoais numa página Internet de uma pessoa singular ou coletiva que alberga o sítio Internet no qual a página pode ser consultada, e que está estabelecida nesse mesmo Estado ou noutro Estado-Membro, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros (n.º 71, disp. 4).

Com efeito, atendendo, por um lado, ao estádio de evolução da Internet à época da elaboração da Diretiva 95/46/CE e, por outro, à ausência de critérios aplicáveis à utilização da Internet no seu capítulo

19 Este acórdão foi apresentado no Relatório Anual de 2003, p. 67.

IV, no qual se insere o referido artigo 25.°, que visa assegurar a fiscalização, pelos Estados-Membros, das transferências de dados pessoais para países terceiros e proibir estas transferências quando estes não ofereçam um nível de proteção adequado, não se pode presumir que o legislador comunitário tinha a intenção de incluir prospetivamente no conceito de «transferência para um país terceiro de dados pessoais» tal inserção de dados numa página Internet, mesmo que deste modo estes se tornem acessíveis às pessoas de países terceiros que possuam os meios técnicos para aceder a esses dados (n.[os] 63, 64, 68).

Acórdão de 6 de outubro de 2015 (Grande Secção), Schrems (C-362/14, EU:C:2015:650) [20]

M. Schrems, cidadão austríaco e utilizador da rede social Facebook, apresentou uma queixa no Data Protection Commissioner (Comissário para a proteção de dados, Irlanda) devido ao facto de a Facebook Ireland transferir os dados pessoais dos seus utilizadores para os Estados Unidos e de os conservar em servidores situados naquele país, onde esses dados eram objeto de um tratamento. Segundo M. Schrems, o direito e as práticas dos Estados Unidos não oferecem uma proteção suficiente contra a vigilância por parte das autoridades públicas dos dados transferidos para esse país. O Data Protection Commissioner tinha recusado investigar sobre essa queixa, designadamente pelo facto de, na Decisão 2000/520/CE [21], a Comissão ter considerado que, no contexto do regime denominado «porto seguro» (em inglês «safe harbour») [22], os Estados Unidos asseguravam um nível de proteção adequado aos dados pessoais transferidos.

Foi neste contexto que o Tribunal de Justiça foi chamado pela High Court (Supremo Tribunal de Justiça, Irlanda) a pronunciar-se sobre um pedido de interpretação do artigo 25.°, n.° 6, da Diretiva 95/46/CE, nos termos do qual a Comissão pode determinar que um país terceiro garante um nível de proteção adequado aos dados transferidos, bem como, em substância, a respeito de um pedido de determinação da validade da Decisão 2000/520/CE adotada pela Comissão com base no artigo 25.°, n.° 6, da Diretiva 95/46/CE.

O Tribunal declarou a decisão da Comissão inválida no seu conjunto, sublinhando, antes de mais, que a sua adoção exigia a constatação devidamente fundamentada por parte da Comissão de que o país terceiro em causa assegurava efetivamente um nível de proteção dos direitos fundamentais substancialmente equivalente ao garantido na ordem jurídica da União. Ora, na medida em que, na sua Decisão 2000/520/CE, a Comissão não procedeu a essa constatação, o artigo 1.° daquela decisão não cumpre os requisitos estabelecidos no artigo 25.°, n.° 6, da Diretiva 95/46/CE, lido à luz da Carta, sendo por esta razão inválido. Com efeito, os princípios de «porto seguro» só se aplicam às organizações americanas autocertificadas que recebam dados pessoais da União, não sendo exigido que as autoridades públicas americanas fiquem sujeitas ao respeito dos referidos princípios. Além do mais, a Decisão 2000/520/CE possibilitava ingerências nos direitos fundamentais das pessoas cujos dados pessoais eram ou podiam ser transferidos da União para os Estados Unidos, sem conter nenhuma referência à existência, nos Estados Unidos, de regras de natureza estatal destinadas a limitar as eventuais ingerências nesses direitos e sem referir a existência de uma proteção jurídica eficaz contra ingerências desta natureza (n.[os] 82, 87-89, 96-98, disp. 2).

Além disso, o Tribunal declarou inválido o artigo 3.° da Decisão 2000/520/CE na medida em que priva as autoridades nacionais de fiscalização dos poderes que o artigo 28.° da Diretiva 95/46/CE lhes conferia nos casos em que uma pessoa apresenta elementos suscetíveis de pôr em causa a compatibilidade com a

20 Este acórdão foi apresentado no Relatório Anual de 2015, p. 53.

21 Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (JO L 215 de 25.8.2000, p. 7).

22 O sistema «porto seguro» inclui um conjunto de princípios relativos à proteção de dados pessoais que as empresas americanas podem subscrever voluntariamente.

proteção da vida privada e das liberdades e direitos fundamentais de uma decisão da Comissão que tenha constatado que um país terceiro assegura um nível de proteção adequado (n.os 102-104). O Tribunal concluiu que a invalidade dos artigos 1.º e 3.º da Decisão 2000/520/CE tinha por efeito afetar a validade desta decisão na sua totalidade (n.os 105, 106).

No que respeita á impossibilidade de justificar tal ingerência, o Tribunal começou por observar que uma regulamentação da União que implique uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta deve prever regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham um mínimo de exigências, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais são sujeitos a um tratamento automático e existe um risco significativo de acesso ilícito aos mesmos (n.º 91).

Além disso, e sobretudo, a proteção do direito fundamental ao respeito da vida privada ao nível da União exige que as derrogações à proteção dos dados pessoais e as suas limitações sejam feitas na estrita medida do necessário (n.º 92). Assim, não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União para os Estados Unidos sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam (n.º 93). Em particular, uma regulamentação que permite às autoridades públicas aceder de forma generalizada ao conteúdo de comunicações eletrónicas infringe o conteúdo essencial do direito fundamental ao respeito pela vida privada. De igual modo, uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, como consagrado no artigo 47.º da Carta (n.os 94, 95).

Parecer 1/15 (Acordo PNR UE-Canadá) de 26 de julho de 2017 (Grande Secção) (EU:C:2017:592)

Em 26 de julho de 2017, o Tribunal de Justiça pronunciou-se pela primeira vez sobre a compatibilidade de um projeto de acordo internacional com a Carta dos Direitos Fundamentais da União Europeia, em particular com as disposições relativas ao respeito pela vida privada e à proteção dos dados pessoais.

A União Europeia e o Canadá negociaram um acordo sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros (PNR) que foi assinado em 2014. O Conselho da União Europeia solicitou ao Parlamento Europeu a sua aprovação, tendo este último decidido recorrer ao Tribunal de Justiça para saber se o acordo previsto era conforme com o direito da União.

O projeto de acordo permite a transferência sistemática e contínua dos dados PNR de todos os passageiros a uma autoridade canadiana para a utilização e o armazenamento, bem como a sua eventual transferência ulterior para outras autoridades e outros países terceiros, com vista a lutar contra o terrorismo e a criminalidade transnacional grave. Para esse efeito, o projeto de acordo prevê, nomeadamente, um período de cinco anos de conservação dos dados e coloca exigências especiais em matéria de segurança e integridade dos PNR, tal como a ocultação imediata dos dados sensíveis, e prevê direitos de acesso, de retificação e de supressão bem como a possibilidade interpor recursos administrativos ou judiciais.

Os dados PNR visados pelo acordo previsto incluem, designadamente, além do nome e dos elementos de contacto do passageiro ou dos passageiros, informações necessárias à reserva, tais como as datas previstas da viagem e o respetivo itinerário, informações sobre os bilhetes, os grupos de pessoas registadas sob o mesmo número de reserva, informações relativas aos meios de pagamento ou à faturação, informações sobre as bagagens e observações gerais acerca dos passageiros.

No seu parecer, o Tribunal declarou que o acordo PNR não pode ser celebrado na sua forma atual devido à incompatibilidade de várias das suas disposições com os direitos fundamentais reconhecidos pela União.

O Tribunal declarou, em primeiro lugar, que tanto a transferência dos dados PNR da União para a autoridade canadiana competente como o enquadramento negociado pela União com o Canadá das condições respeitantes ao período de conservação desses dados, à sua utilização e à sua transferência ulterior para outras autoridades canadianas, à Europol, ao Eurojust, às autoridades policiais ou judiciais dos Estados-Membros ou ainda às autoridades de outros países terceiros, constituem uma ingerência no direito garantido pelo artigo 7.º da Carta. Estas operações são igualmente constitutivas de uma ingerência no direito fundamental à proteção dos dados pessoais garantido pelo artigo 8.º da Carta, visto que constituem tratamentos dos dados pessoais (n.os 125, 126).

Além disso, o Tribunal sublinhou que, embora alguns dos dados PNR, tomados isoladamente, não pareçam suscetíveis de revelar informações importantes sobre a vida provada das pessoas em causa, o certo é que, considerados conjuntamente, os referidos dados podem, entre outros, revelar um itinerário de viagem completo, hábitos de viagem, relações existentes entre duas ou mais pessoas e informações sobre a situação financeira dos passageiros aéreos, os seus hábitos alimentares ou o seu estado de saúde, podendo até fornecer informações sensíveis sobre esses passageiros, conforme definidas no artigo 2.º, alínea e), do acordo projetado (informações que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas, etc.) (n.º 128).

A este respeito, o Tribunal considerou que, embora as intervenções em causa possam ser justificadas pela prossecução de um objetivo de interesse geral (garantia da segurança pública no âmbito da luta contra as infrações terroristas e a criminalidade transnacional grave), várias disposições do Acordo não são limitadas ao estritamente necessário e não preveem regras claras e precisas.

Em especial, o Tribunal salientou que, tendo em conta o risco de um tratamento contrário ao princípio da não discriminação, a transferência de dados sensíveis para o Canadá exigiria uma justificação precisa e particularmente sólida, baseada em fundamentos diferentes da proteção da segurança pública contra o terrorismo e a criminalidade transnacional grave. Ora, neste caso, tal justificação não existe. O Tribunal concluiu que as disposições do acordo sobre a transferência de dados sensíveis para o Canadá, bem como sobre o tratamento e a conservação desses dados são incompatíveis com os direitos fundamentais (n.os 165, 232).

Em segundo lugar, o Tribunal considerou que, após a partida dos passageiros aéreos do Canadá, o armazenamento contínuo dos dados PNR de todos os passageiros aéreos permitido pelo acordo projetado não se limita ao estritamente necessário. Com efeito, no que se refere aos passageiros aéreos em relação aos quais, à sua chegada ao Canadá e até à sua saída deste país, não foi identificado um risco em matéria de terrorismo ou criminalidade transnacional grave, não se afigura existir, uma vez saídos desse país, nenhuma relação, ainda que indireta, entre os seus dados PNR e o objetivo prosseguido pelo acordo projetado, que justifique a conservação destes dados. Em contrapartida, o armazenamento dos dados PNR relativos a passageiros aéreos relativamente aos quais são identificados elementos objetivos que permitem considerar que, mesmo após a sua partida do Canadá, os mesmos podem apresentar um risco em termos de luta contra o terrorismo e a criminalidade transnacional grave é admissível para além da sua estada nesse país, mesmo por um período de cinco anos (n.os 205-207, 209).

Em terceiro lugar, o Tribunal declarou que o direito fundamental ao respeito pela vida privada, consagrado no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia, implica que a pessoa em causa possa certificar-se de que esses dados pessoais são tratados com exatidão e de forma lícita. Para poder efetuar as verificações necessárias, essa pessoa deve dispor de um direito de acesso aos dados que lhe digam respeito que são objeto de um tratamento.

A este respeito, o Tribunal sublinhou que, no acordo projetado, importa que os passageiros aéreos sejam informados da transferência dos seus dados dos registos de identificação dos passageiros para o país terceiro em causa e da utilização de tais dados a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo pelas autoridades públicas a que se aplica o acordo projetado. Com efeito, essa informação é, de facto, necessária para permitir aos passageiros aéreos exercer os seus direitos de pedir o acesso aos dados que lhes dizem respeito e, sendo caso disso, a retificação dos mesmos, bem como intentar, em conformidade com o artigo 47.º, primeiro parágrafo, da Carta, uma ação perante um tribunal.

Assim, nas hipóteses em que existem elementos objetivos que justificam a utilização dos dados dos registos de identificação dos passageiros para lutar contra o terrorismo e a criminalidade transnacional grave e que carecem de uma autorização prévia de uma autoridade judiciária ou de uma entidade administrativa independente, afigura-se necessária uma informação individual dos passageiros. O mesmo se diga dos casos em que os dados PNR dos passageiros aéreos são comunicados a outras autoridades públicas ou a particulares. No entanto, tal informação apenas deve ocorrer a partir do momento em que não seja suscetível de comprometer as investigações levadas a cabo pelas autoridades públicas previstas no acordo projetado (n.os 219, 220, 223, 224).

IV. A proteção dos dados pessoais na Internet

1. Direito de oposição ao tratamento dos dados pessoais («direito de ser esquecido»)

Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317)

Neste acórdão (ver também rubrica II.3, intitulada «Conceito de 'tratamento de dados pessoais'»), o Tribunal de Justiça precisou o alcance dos direitos de acesso e de oposição ao tratamento de dados pessoais na Internet, previstos pela Diretiva 95/46/CE.

Assim, quando se pronunciou sobre a questão do alcance da responsabilidade do operador de um motor de busca na Internet, o Tribunal declarou, em substância, que, para respeitar os direitos de acesso e oposição garantidos pelos artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46/CE, e desde que as condições previstas nesses artigos estejam reunidas, este é, em certas circunstâncias, obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a páginas web publicadas por terceiros e que contenham informações sobre essa pessoa. O Tribunal precisou que essa obrigação também pode existir na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita (n.º 88, disp. 3).

Por outro lado, interrogado sobre a questão de saber se a diretiva permite que a pessoa em causa solicite que ligações a páginas web sejam suprimidas de uma lista de resultados com o fundamento de que

pretende que as informações que aí figuram relativas à sua pessoa sejam «esquecidas» após um certo período de tempo, o Tribunal salienta, em primeiro lugar, que mesmo um tratamento inicialmente lícito de dados exatos se pode tornar, com o tempo, incompatível com esta diretiva, quando esses dados já não sejam necessários atendendo às finalidades para que foram recolhidos ou tratados, designadamente, quando são objetivamente inadequados, quando não são pertinentes ou já não são pertinentes ou quando são excessivos atendendo a essas finalidades ou ao tempo decorrido (n.º 93). Assim, caso se conclua, no seguimento de um pedido da pessoa em causa, que a inclusão dessas ligações na lista é, na situação atual, incompatível com a diretiva, as informações e ligações que figuram nesta lista devem ser suprimidas (n.º 94). Neste contexto, a constatação de um direito da pessoa em causa a que a informação sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados não pressupõe que a inclusão da informação em questão na lista de resultados cause prejuízo à pessoa em causa (n.º 96, disp. 4).

Finalmente, o Tribunal indicou que, na medida em que a pessoa em causa pode, tendo em conta os seus direitos fundamentais ao abrigo dos artigos 7.º e 8.º da Carta, requerer que a informação em questão deixe de estar à disposição do grande público através da sua inclusão numa lista de resultados deste tipo, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais, como o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão em virtude dessa inclusão (n.º 97, disp. 4).

2. Tratamento dos dados pessoais e direitos de propriedade intelectual

Acórdão de 29 de janeiro de 2008 (Grande Secção), Promusicae (C-275/06, EU:C:2008:54) [23]

A Promusicae, uma associação espanhola sem fins lucrativos que agrupa produtores e editores de gravações musicais e audiovisuais, tinha recorrido aos tribunais espanhóis para que a Telefónica de España SAU (sociedade comercial que tem como atividade, nomeadamente, a prestação de serviços de acesso à Internet) fosse intimada a revelar a identidade e o endereço físico de certas pessoas a quem esta última prestava serviços de acesso à Internet e cujo endereço IP e a data e hora da ligação eram conhecidas. Segundo a Promusicae, essas pessoas utilizavam o programa de troca de ficheiros dito «peer-to-peer» ou «P2P» (meio transparente de partilha de conteúdos, independente, descentralizado e munido de funções de busca e de descarga avançadas) e permitiam o acesso, nos ficheiros partilhados dos respetivos computadores pessoais, a fonogramas cujos direitos patrimoniais de exploração pertenciam aos sócios da Promusicae. Assim, pedia que lhe fossem transmitidas essas informações para poder propor ações cíveis contra os interessados.

Nestas condições, o Juzgado de lo Mercantil n.º 5 de Madrid (Tribunal de Comércio n.º 5 de Madrid, Espanha) submeteu ao Tribunal de Justiça a questão de saber se a legislação europeia impõe aos Estados-Membros que prevejam, para garantir a efetiva proteção dos direitos de autor, a obrigação de transmitir dados de caráter pessoal no âmbito de uma ação cível.

Segundo o Tribunal, o referido pedido de decisão prejudicial suscitou a questão da necessária conciliação entre as exigências ligadas à proteção de diferentes direitos fundamentais, a saber, por um lado, o direito ao respeito pela vida privada, e, por outro, os direitos à proteção da propriedade e a uma tutela jurisdicional efetiva.

23 Este acórdão foi apresentado no Relatório Anual de 2008, p. 46.

A este respeito, o Tribunal concluiu que as Diretivas 2000/31/CE, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») [24], 2001/29/CE, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação [25], 2004/48/CE, relativa ao respeito dos direitos de propriedade intelectual [26], e 2002/58/CE não impõem aos Estados-Membros que prevejam, numa situação como a do processo principal, a obrigação de transmitir dados pessoais para garantir a efetiva proteção do direito de autor no âmbito de uma ação cível. Porém, o direito da União exige que os referidos Estados, na transposição dessas diretivas, providenciem no sentido de ser seguida uma interpretação das mesmas que permita assegurar um justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária. Em seguida, ao darem execução às medidas de transposição das referidas diretivas, incumbe às autoridades e aos órgãos jurisdicionais dos Estados-Membros não apenas interpretar o seu direito nacional em conformidade com essas mesmas diretivas, mas também seguir uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o princípio da proporcionalidade (n.º 70 e disp.).

Acórdão de 24 de novembro de 2011, Scarlet Extended (C-70/10, EU:C:2011:771) [27]

A sociedade belga de autores, compositores e editores SCRL (SABAM) constatou que os internautas que utilizam os serviços da Scarlet Extended SA, um fornecedor de acesso à Internet (a seguir «Scarlet»), descarregavam na Internet, sem autorização e sem pagar direitos, obras constantes do seu catálogo através de redes «peer-to-peer». A SABAM intentou uma ação no tribunal nacional, o qual, em primeira instância, julgou procedente a sua pretensão e intimou a Scarlet a pôr termo a essas violações dos direitos de autor tornando impossível, através de um software «peer-to-peer», qualquer forma de envio ou de receção pelos seus clientes de ficheiros eletrónicos contendo uma obra musical do repertório da SABAM.

Chamada a conhecer do processo pela Scarlet, a cour d'appel de Bruxelles (Tribunal de Recurso de Bruxelas, Bélgica) suspendeu a instância para perguntar ao Tribunal de Justiça, a título prejudicial, se tal medida inibitória era compatível com o direito europeu.

O Tribunal declarou que as Diretivas 95/46/CE, 2000/31/CE, 2001/29/CE, 2002/58/CE e 2004/48/CE, lidas conjuntamente e interpretadas à luz das exigências resultantes da proteção dos direitos fundamentais aplicáveis, devem ser interpretadas no sentido de que se opõem a uma medida inibitória que intima a Scarlet a criar um sistema de filtragem de todas as comunicações eletrónicas que transitam pelos seus serviços, nomeadamente através da utilização de software «peer-to-peer», aplicável indistintamente a toda a sua clientela, com caráter preventivo, a expensas suas e sem limitação no tempo, e que seja apta a identificar na rede desse fornecedor a circulação de ficheiros eletrónicos que contenham uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega ser titular de direitos de propriedade intelectual, com o objetivo de bloquear a transferência de ficheiros cujo intercâmbio viole os direitos de autor (n.º 54 e disp.).

Com efeito, segundo o Tribunal, uma tal medida inibitória não respeita a proibição, imposta pelo artigo 15.º, n.º 1, da Diretiva 2000/31/CE, de impor a esse prestador de serviços uma obrigação geral de vigilância, nem a exigência de assegurar o justo equilíbrio entre, por um lado, o direito de propriedade

24 Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).

25 Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de maio de 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação (JO L 167 de 22.6.2001, p. 10).

26 Diretiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao respeito dos direitos de propriedade intelectual (JO L 157, p. 45 de 30.04.2004, e retificação no JO L 195, de 2.6.2004, p. 16);

27 Este acórdão foi apresentado no Relatório Anual de 2011, p. 37.

intelectual e, por outro, a liberdade de empresa e o direito à proteção dos dados pessoais, bem como a liberdade de receber ou de transmitir informações (n.os 40,49).

Neste contexto, o Tribunal salientou que, por um lado, a medida inibitória que ordena a instalação do sistema de filtragem controvertido implicaria uma análise sistemática de todos os conteúdos e a recolha e identificação dos endereços IP dos utilizadores que estão na origem do envio de conteúdos ilícitos na rede, sendo esses endereços dados pessoais protegidos, uma vez que permitem a identificação precisa dos referidos utilizadores. Por outro lado, haveria o risco de a referida medida inibitória violar a liberdade de informação, dado que esse sistema poderia não distinguir suficientemente um conteúdo ilícito de um lícito, de modo que o seu acionamento poderia provocar o bloqueio de comunicações de conteúdo lícito. Com efeito, não é contestado que a resposta à questão da licitude de uma transmissão depende igualmente da aplicação de exceções legais aos direitos de autor que variam de um Estado-Membro para outro. Além disso, em certos Estados-Membros, certas obras podem pertencer ao domínio público ou os autores em causa podem colocá-las gratuitamente à disposição do público na Internet (n.° 52).

Consequentemente, o Tribunal declarou que, ao adotar a medida inibitória que obriga a Scarlet a instalar o sistema de filtragem controvertido, o órgão jurisdicional nacional não respeitou a exigência de assegurar um justo equilíbrio entre o direito de propriedade intelectual, por um lado, e a liberdade de empresa, o direito à proteção dos dados pessoais e a liberdade de receber ou de enviar informações, por outro (n.° 53).

Acórdão de 19 de abril de 2012, Bonnier Audio e o. (C-461/10, EU:C:2012:219)

O Högsta domstolen (Supremo Tribunal, Suécia) submeteu um pedido prejudicial ao Tribunal de Justiça com vista à interpretação das Diretivas 2002/58/CE e 2004/48/CE, no âmbito de um litígio que opõe a Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB e a Storyside AB (a seguir «Bonnier Audio e o.») à Perfect Communication Sweden AB (a seguir «ePhone») a respeito da oposição desta última a um pedido de injunção para comunicação de dados apresentado pela Bonnier Audio e o.

No caso em apreço, a Bonnier Audio e o. eram sociedades editoras, titulares, nomeadamente, de direitos exclusivos de reprodução, edição e colocação à disposição do público de 27 obras que se apresentavam sob a forma de audiolivros. Consideravam que os seus direitos exclusivos tinham sido violados devido à difusão ao público dessas 27 obras, sem o seu consentimento, por meio de um servidor FTP («file transfer protocol») que permitia a partilha de ficheiros e a transmissão de dados entre computadores ligados à Internet. Por conseguinte, apresentaram aos tribunais suecos um pedido de injunção para comunicação do nome e endereço da pessoa que utilizava o endereço IP a partir do qual se presumia que os ficheiros em causa tinham sido transmitidos.

Neste contexto, o Högsta domstolen, chamado a conhecer do recurso, interrogou o Tribunal de Justiça sobre a questão de saber se o direito da União obsta à aplicação de uma disposição nacional adotada com base no artigo 8.° da Diretiva 2004/48 que, com o objetivo de identificar um assinante, permite que se imponha a um fornecedor de Internet a obrigação de comunicar ao titular de um direito de autor, ou aos seus sucessores, no âmbito de um processo civil, a identidade do assinante a quem foi atribuído um endereço IP e a partir do qual foi praticada a violação do referido direito. A questão pressupunha, por um lado, que o requerente da injunção tinha reunido indícios reais de violação de um direito de autor e, por outro lado, que a medida era proporcionada.

O Tribunal começou por recordar que o artigo 8.°, n.° 3, da Diretiva 2004/48/CE, lido em conjugação com o artigo 15.°, n.° 1, da Diretiva 2002/58/CE, não se opõe a que os Estados-Membros prevejam uma obrigação de transmissão de dados pessoais a entidades privadas a fim de permitir desencadear, nas instâncias cíveis, um procedimento judicial contra as violações dos direitos de autor, mas também não obriga esses Estados a prever essa obrigação. No entanto, incumbe às autoridades e aos órgãos

jurisdicionais dos Estados-Membros não só interpretar o seu direito nacional em conformidade com estas mesmas diretivas mas também providenciar no sentido de ser seguida uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito da União, como o princípio da proporcionalidade (n.os 55, 56).

A este respeito, foi constatado que a legislação nacional em questão exigia, nomeadamente, que, para que pudesse ser ordenada uma intimação de comunicação dos dados em causa, existissem indícios reais de violação de um direito de propriedade intelectual sobre uma obra, que as informações pedidas fossem suscetíveis de facilitar a investigação sobre a violação do direito de autor ou a lesão desse direito e que as razões que justificavam essa intimação fossem de interesse superior aos inconvenientes ou aos outros prejuízos que a mesma pudesse ocasionar ao seu destinatário ou a qualquer interesse que se lhe opusesse (n.º 58).

Por conseguinte, o Tribunal concluiu que as Diretivas 2002/58/CE e 2004/48/CE não se opõem a uma legislação nacional como a que estava em causa no processo principal, na medida em que esta legislação permite ao órgão jurisdicional nacional ao qual uma pessoa com legitimidade ativa apresentou um pedido de intimação para comunicação de dados pessoais, ponderar os interesses opostos envolvidos em função das circunstâncias de cada caso e tendo em devida conta as exigências decorrentes do princípio da proporcionalidade (n.º 61 e disp).

V. Autoridades nacionais de fiscalização

1. Alcance da exigência de independência

Acórdão de 9 de março de 2010 (Grande Secção), Comissão/Alemanha (C-518/07, EU:C:2010:125) [28]

Na sua petição, a Comissão pedia ao Tribunal de Justiça que declarasse que a República Federal da Alemanha, ao submeter à tutela do Estado as autoridades de fiscalização competentes para fiscalizar o tratamento de dados pessoais no setor não público nos diferentes Länder, transpondo, assim, de forma errada a exigência de «total independência» das autoridades encarregadas de garantir a proteção desses dados, não cumpriu as obrigações que lhe incumbem por força do artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46/CE.

A República Federal da Alemanha, por seu turno, considerava que o artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46/CE exige uma independência funcional das autoridades de fiscalização, no sentido de que essas autoridades devem ser independentes do setor não público sujeito à sua fiscalização e não devem estar expostas a influências externas. Ora, na sua opinião, a tutela do Estado exercida nos Landër alemães não constituía uma tal influência externa, tratando-se antes de um mecanismo de vigilância interna da Administração, instituído por autoridades que fazem parte do mesmo aparelho administrativo que as autoridades de fiscalização e que estão obrigadas, como estas autoridades, a cumprir os objetivos da Diretiva 95/46/CE.

O Tribunal declarou que a garantia de independência das autoridades nacionais de fiscalização prevista na Diretiva 95/46/CE visa assegurar a eficácia e a fiabilidade da fiscalização do respeito das disposições em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e

28 Este acórdão foi apresentado no Relatório Anual de 2010, p. 34.

deve ser interpretada à luz deste objetivo. Não foi estabelecida para conferir um estatuto especial às próprias autoridades e aos seus agentes, mas com vista a reforçar a proteção das pessoas e dos organismos abrangidos pelas suas decisões, sendo que as autoridades de supervisão devem, portanto, no exercício das suas funções, agir de forma objetiva e imparcial (n.º 25).

O Tribunal considerou que essas autoridades de fiscalização competentes para fiscalizar o tratamento dos dados pessoais no setor não público devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Essa independência exclui não só qualquer influência exercida pelos organismos de fiscalização mas também qualquer instrução ou qualquer outra influência externa, direta ou indireta, que possam pôr em causa o cumprimento, pelas referidas autoridades, da sua tarefa de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação de dados pessoais. O mero risco de as autoridades de tutela poderem exercer uma influência política nas decisões das autoridades de fiscalização é suficiente para impedir o exercício independente das suas funções. Por um lado, daí poderia resultar uma «obediência antecipada» dessas autoridades atendendo à prática decisória da autoridade de tutela. Por outro lado, o papel de guardiãs do direito à vida privada que as referidas autoridades de fiscalização desempenham exige que as suas decisões e, consequentemente, elas próprias, estejam acima de qualquer suspeita de parcialidade. Segundo o Tribunal, a tutela do Estado exercida sobre as autoridades nacionais de fiscalização não é, por conseguinte, compatível com a exigência de independência (n.^{os} 30, 36, 37 e disp.).

Acórdão de 16 de outubro de 2012 (Grande Secção) Comissão/Áustria (C-614/10, EU:C:2012:631)

Na sua petição, a Comissão pediu ao Tribunal de Justiça que declarasse que, ao não adotar todas as disposições necessárias para que a legislação em vigor na Áustria cumprisse o critério de independência no que respeita à Datenschutzkommission (Comissão para a proteção dos dados), instituída como autoridade de fiscalização da proteção de dados pessoais, a Áustria não cumpriu as obrigações que lhe incumbem por força do artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46/CE.

O Tribunal constatou um incumprimento por parte da Áustria, considerando, em substância, que não cumpre o critério de independência da autoridade de fiscalização, estabelecido pela Diretiva 95/46/CE, o Estado-Membro que institui um quadro regulamentar ao abrigo do qual o membro administrador da referida autoridade é um funcionário do Estado, sujeito a supervisão, cujo gabinete está integrado nos serviços do governo nacional, e relativamente à qual o chefe do governo nacional dispõe de um direito incondicional à informação sobre todos os aspetos da sua gestão (n.º 66 e disp).

O Tribunal recordou, antes de mais, que a expressão «com total independência» constante do artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46/CE, implicam que as autoridades de fiscalização devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Neste aspeto, o facto de essa autoridade beneficiar de uma independência funcional na medida em que os seus membros são independentes e não estão vinculados por nenhuma instrução no exercício da sua função não basta, por si só, para preservar a autoridade de fiscalização de qualquer influência externa. Ora, a independência exigida neste contexto visa excluir não só a influência direta, sob a forma de instruções, mas também qualquer forma de influência indireta suscetível de orientar as decisões da autoridade de fiscalização. Por outro lado, o papel de guardiãs do direito à vida privada que as referidas autoridades desempenham exige que as suas decisões e, consequentemente, elas próprias, estejam acima de qualquer suspeita de parcialidade (n.^{os} 41-43, 52).

O Tribunal precisou que, para poder cumprir o critério de independência enunciado na referida disposição da Diretiva 95/46/CE, uma autoridade nacional de fiscalização não deve dispor de uma rubrica orçamental autónoma, à semelhança da prevista no artigo 43.º, n.º 3, do Regulamento (CE) n.º 45/2001. Com efeito, os Estados-Membros não são obrigados a reproduzir, na sua legislação nacional, disposições

análogas às do capítulo V do Regulamento (CE) n.º 45/2001 para garantir uma independência total à(s) sua(s) autoridade(s) de fiscalização, pelo que podem prever que, do ponto de vista orçamental, a autoridade de fiscalização depende de um determinado departamento ministerial. Contudo, a atribuição dos meios humanos e materiais necessários a essa autoridade não deve impedi-la de exercer as suas funções «com total independência» na aceção do artigo 28.º, n.º 1, segundo parágrafo, da Diretiva 95/46/CE (n.º 58).

Acórdão de 8 de abril de 2014 (Grande Secção), Comissão/Hungria (C-288/12, EU:C:2014:237) [29]

Neste processo, a Comissão pedia ao Tribunal que declarasse que, ao fazer cessar antecipadamente o mandato da autoridade de fiscalização da proteção de dados pessoais, a Hungria não cumpriu as obrigações que lhe incumbem por força da Diretiva 95/46/CE.

O Tribunal declarou que um Estado-Membro que faz cessar antecipadamente o mandato da autoridade de fiscalização da proteção de dados pessoais não cumpre as obrigações que lhe incumbem por força da Diretiva 95/46/CE (n.º 62, disp. 1).

Com efeito, segundo o Tribunal, a independência de que devem gozar as autoridades de fiscalização competentes para a supervisão do tratamento dos referidos dados exclui, designadamente, qualquer instrução e qualquer outra influência externa, sob qualquer forma, seja direta ou indireta, suscetíveis de orientar as suas decisões e que podem assim pôr em causa o cumprimento, pelas referidas autoridades, da sua função de estabelecer um justo equilíbrio entre a proteção da vida privada e a livre circulação dos dados de natureza pessoal (n.º 51).

Além disso, o Tribunal recordou que, na medida em que a independência funcional não basta, por si só, para resguardar as autoridades de fiscalização de qualquer influência externa, o mero risco de as autoridades de tutela de um Estado poderem exercer uma influência política nas decisões das autoridades de fiscalização é suficiente para impedir o exercício independente das funções destas. Ora, se cada Estado-Membro pudesse fazer cessar o mandato de uma autoridade de fiscalização antes do termo inicialmente previsto, sem respeitar as regras e garantias previamente estabelecidas para esse efeito pela legislação aplicável, a ameaça dessa cessação antecipada que pairaria sobre essa autoridade ao longo do exercício do seu mandato poderia levar a uma forma de obediência desta ao poder político, incompatível com a referida exigência de independência. Além disso, nessa situação, não se pode considerar que a autoridade de fiscalização pode, em qualquer circunstância, operar acima de qualquer suspeita de parcialidade (n.os 52-55).

2. Determinação do direito aplicável e da autoridade de fiscalização competente

Acórdão de 1 de outubro de 2015, Weltimmo (C-230/14, EU:C:2015:639) [30]

A Nemzeti Adatvédelmi és Információszabadság Hatóság (Autoridade nacional para a proteção dos dados e a liberdade de informação, Hungria) aplicou uma coima à Weltimmo, sociedade registada na Eslováquia, que explorava sítios Internet de anúncios imobiliários de bens situados na Hungria, pelo facto de esta não ter apagado os dados pessoais dos anunciantes desses sítios, apesar do pedido destes nesse sentido, e pelo facto de aquela sociedade ter comunicado esses dados a agências de recuperação de crédito com vista a obter o pagamento de faturas não pagas. Segundo a autoridade de fiscalização

29 Este acórdão foi apresentado no Relatório Anual de 2010, p. 34.
30 Este acórdão foi apresentado no Relatório Anual de 2015, p. 55.

húngara, a empresa Weltimmo tinha, desse modo, violado a legislação húngara que transpõe a Diretiva 95/46/CE.

Chamada a conhecer de um recurso, a Kúria (Supremo Tribunal, Hungria) teve dúvidas quanto à determinação do direito aplicável e dos poderes de que dispõe a autoridade de fiscalização húngara com base nos artigos 4.°, n.° 1, e artigo 28.° da Diretiva 95/46/CE. Por conseguinte, submeteu várias questões prejudiciais ao Tribunal de Justiça.

No que respeita ao direito nacional aplicável, o Tribunal declarou que o artigo 4.°, n.° 1, alínea a), da Diretiva 95/46/CE permite a aplicação da legislação relativa à proteção dos dados pessoais de um Estado-Membro diferente daquele em que o responsável pelo tratamento desses dados está registado, desde que este exerça, através de uma instalação estável no território desse Estado-Membro, uma atividade efetiva e real, ainda que mínima, em cujo contexto esse tratamento é efetuado. Para determinar se é esse o caso, o órgão jurisdicional de reenvio pode, designadamente, ter em conta, por um lado, que a atividade do responsável pelo referido tratamento, no âmbito da qual este último tenha lugar, consiste na exploração de sítios Internet de anúncios de imobiliários de bens situados no território desse Estado-Membro e que tenham sido redigidos na língua deste e que, por conseguinte, é principalmente, ou mesmo totalmente, direcionada para esse Estado-Membro. Por outro lado, o órgão jurisdicional de reenvio também pode ter em conta o facto de esse responsável dispor de um representante no referido Estado-Membro, encarregado de cobrar os créditos resultantes dessa atividade e de representá-lo em processos administrativos e judiciais relativos ao tratamento dos dados em causa. Em contrapartida, o Tribunal considerou que a questão da nacionalidade das pessoas afetadas por esse tratamento de dados é desprovida de pertinência (n.° 41, disp. 1).

No que respeita à competência e aos poderes da autoridade de fiscalização à qual tenham sido apresentadas queixas, em conformidade com o artigo 28.°, n.° 4, da Diretiva 95/46/CE, o Tribunal considerou que esta autoridade pode analisar essas queixas independentemente do direito aplicável e inclusivamente antes de saber qual é o direito nacional aplicável ao tratamento em causa (n.° 54). No entanto, se concluir que é aplicável o direito de outro Estado-Membro, não poderá aplicar sanções fora do território do Estado-Membro a que pertence. Nessa situação, cabe-lhe, em aplicação do dever de cooperação previsto no artigo 28.°, n.° 6, da mesma diretiva, pedir à autoridade de fiscalização desse outro Estado-Membro que verifique a existência de uma eventual infração a esse direito e que aplique sanções se este último o permitir, baseando-se, se for caso disso, nas informações que lhe tiver transmitido (n.os 57, 60, disp. 2).

3. Poderes das autoridades nacionais de fiscalização

Acórdão de 6 de outubro de 2015 (Grande secção) Schrems (C-362/14, EU:C:2015:650)

Neste processo (ver também a rubrica III, intitulada «Transferência de dados pessoais para países terceiros»), o Tribunal de Justiça declarou nomeadamente que as autoridades nacionais de fiscalização são competentes para controlar as transferências de dados pessoais para países terceiros.

A este respeito, o Tribunal começou por constatar que as autoridades nacionais de fiscalização dispõem de um amplo leque de poderes, enumerados de forma não exaustiva no artigo 28.°, n.° 3, da Diretiva 95/46/CE, que constituem os meios necessários para o desempenho das suas funções. Assim, as referidas autoridades gozam, nomeadamente, de poderes de inquérito, tais como recolher todas as informações necessárias ao desempenho das suas funções de fiscalização, de poderes efetivos de intervenção, tais como proibir temporária ou definitivamente um tratamento de dados ou ainda do poder de intervir em processos judiciais (n.° 43).

No que diz respeito ao poder de controlar as transferências de dados pessoais para os países terceiros, o Tribunal declarou que é certo que decorre do artigo 28.°, n.os 1 e 6, da Diretiva 95/46/CE que os poderes das autoridades nacionais de fiscalização respeitam aos tratamentos de dados pessoais efetuados no território do Estado-Membro dessas autoridades, pelo que não dispõem de poderes, ao abrigo deste artigo 28.°, relativamente aos tratamentos de tais dados efetuados no território de um país terceiro (n.° 44).

No entanto, a operação que consiste em transferir dados pessoais a partir de um Estado-Membro para um país terceiro constitui, enquanto tal, um tratamento de dados pessoais efetuado no território de um Estado-Membro. Por conseguinte, uma vez que as autoridades nacionais de fiscalização estão encarregadas, em conformidade com o artigo 8.°, n.° 3, da Carta e com o artigo 28.° da Diretiva 95/46/CE, da fiscalização do cumprimento das regras da União relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, cada uma delas tem competência para verificar se uma transferência de dados pessoais do Estado-Membro dessa autoridade para um país terceiro respeita as exigências estabelecidos por esta diretiva (n.os 45, 47).

VI. Aplicação territorial da legislação europeia

Acórdão de 13 de maio de 2014 (Grande Secção), Google Spain e Google (C-131/12, EU:C:2014:317)

Neste acórdão (ver também a rubrica II.3, intitulada «Conceito de 'tratamento de dados pessoais'», e IV.1, intitulada «Direito de oposição ao tratamento dos dados pessoais ('direito de ser esquecido')»), o Tribunal de Justiça também se pronunciou sobre o âmbito de aplicação geográfico da Diretiva 95/46/CE.

Assim, o Tribunal declarou que é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro, na aceção da Diretiva 95/46/CE, quando o operador de um motor de busca, ainda que tenha a sua sede num Estado terceiro, cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro (n.os 55, 60, disp. 2).

Com efeito, nestas circunstâncias, as atividades do operador do motor de busca e as do seu estabelecimento situado num Estado-Membro, embora distintas, estão indissociavelmente ligadas, uma vez que as atividades relativas aos espaços publicitários constituem o meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades (n.os 56).

VII. Direito de acesso do público aos documentos das instituições da União Europeia e proteção dos dados pessoais

Acórdão de 29 de junho de 2010 (Grande Secção), Comissão/Bavarian Lager (C-28/08 P, EU:C:2010:378)

A Bavarian Lager, sociedade criada para importar cerveja alemã para venda em estabelecimentos de bebidas no Reino Unido, não pôde vender o seu produto, uma vez que um grande número de

empresários de estabelecimentos de venda de bebidas do Reino Unido estavam vinculados por contratos de compra exclusiva que os obrigavam a abastecer-se de cerveja junto de certos fabricantes de cerveja.

Por força da regulamentação do Reino Unido relativa ao fornecimento de cerveja (a seguir «GBP»), os fabricantes de cerveja britânicos eram obrigados a conceder aos gerentes dos pubs a possibilidade de comprarem uma cerveja proveniente de outra fábrica, na condição de ser acondicionada em barril. Ora, a maior parte das cervejas produzidas fora do Reino Unido não podiam ser consideradas «cervejas vendidas em barril», na aceção da GBP, e, por conseguinte, não se enquadravam no seu âmbito de aplicação. Considerando que a referida regulamentação constituía uma medida de efeito equivalente a uma restrição quantitativa às importações, a Bavarian Lager apresentou uma denúncia à Comissão.

Durante o processo por incumprimento iniciado pela Comissão contra o Reino Unido, os representantes das administrações comunitária e britânica, bem como representantes da Confederação dos fabricantes de cerveja do mercado comum (CBMC), participaram numa reunião que decorreu em 11 de outubro de 1996. Depois de ter sido informada pelas autoridades inglesas da alteração da regulamentação em causa no sentido de permitir a venda de cerveja engarrafada como cerveja de proveniência diferente, como a cerveja em barril, a Comissão informou a Bavarian Lager da suspensão do processo por incumprimento.

A Bavarian Lager apresentou um pedido com vista a obter a ata completa da reunião de outubro de 1996, com a menção do nome de todos os participantes, o qual foi indeferido pela Comissão por decisão de 18 de março de 2004, com fundamento, nomeadamente, na proteção da vida privada, como garantida pelo regulamento relativo à proteção dos dados pessoais.

A Bavarian Lager interpôs um recurso no Tribunal Geral no qual pedia a anulação desta decisão da Comissão. Por acórdão de 8 de novembro de 2007, o Tribunal Geral anulou a decisão da Comissão, considerando, nomeadamente, que a simples inscrição do nome dos interessados na lista das pessoas que participaram numa reunião em nome da entidade que representavam não lesava os interesses nem comprometia a vida privada dessas pessoas. A Comissão, apoiada pelo Reino Unido e pelo Conselho, interpôs no Tribunal de Justiça um recurso deste acórdão do Tribunal Geral.

O Tribunal de Justiça começou por observar que, quando um pedido baseado no Regulamento (CE) n.º 1049/2001 [31], relativo ao acesso aos documentos, se destina a obter o acesso a documentos que incluem dados pessoais, as disposições do Regulamento (CE) n.º 45/2001 passam a ser integralmente aplicáveis, incluindo a disposição que impõe ao destinatário da transferência de dados pessoais a obrigação de demonstrar a necessidade da sua divulgação e a disposição que confere à pessoa em causa a possibilidade de se opor em qualquer momento, por razões imperiosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de um tratamento (n.º 63).

Em seguida, o Tribunal declarou que a lista dos participantes numa reunião realizada no âmbito de um processo por incumprimento que figuram na ata da referida reunião continha dados pessoais, na aceção do artigo 2.º, alínea a), do Regulamento (CE) n.º 45/2001, uma vez que as pessoas que participaram nesta reunião podiam ser identificadas (n.º 70).

Por último, concluiu que, ao exigir que, relativamente às pessoas que não deram o seu consentimento expresso à divulgação dos dados pessoais que lhes diziam respeito contidas neste relatório, a necessidade da transferência desses dados pessoais fosse demonstrada, a Comissão tinha dado cumprimento às disposições do artigo 8.º, alínea b), do referido regulamento (n.º 77).

31 Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

Com efeito, quando, no âmbito de um pedido de acesso à referida ata ao abrigo do Regulamento (CE) n.º 1049/2001, não é fornecida nenhuma justificação expressa e legítima nem nenhum argumento convincente para demonstrar a necessidade da transferência desses dados pessoais, a Comissão não pode ponderar os diferentes interesses das partes em causa. A comissão também não podia verificar se não existiam motivos para supor que os interesses legítimos das pessoas em causa podiam ser lesados, como prevê o artigo 8.º, alínea b), do Regulamento n.º 45/2001 (n.º 78) [32].

Processo de 16 de julho de 2015, ClientEarth e PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

A Autoridade Europeia para a Segurança dos Alimentos (EFSA) constituiu um grupo de trabalho a fim de elaborar uma orientação para indicar a maneira de aplicar o artigo 8.º, n.º 5, do Regulamento (CE) n.º 1107/2009 [33], nos termos do qual o autor de um pedido de autorização de colocação no mercado de um produto fitofarmacêutico deve juntar ao processo a literatura científica existente, como determinada pela EFSA, validada pela comunidade científica, sobre os efeitos secundários da substância ativa e dos seus metabolitos relevantes na saúde, no ambiente e nas espécies não visadas.

O projeto de orientação foi submetido a consulta pública, tendo a ClientEarth e a Pesticide Action Network Europe (PAN Europe) apresentado observações sobre o projeto. Neste contexto, apresentaram conjuntamente à EFSA um pedido de acesso a documentos relativos à preparação do projeto de orientação, incluindo as observações dos peritos externos.

A EFSA autorizou a ClientEarth e a PAN Europe a acederem, nomeadamente, às observações individuais dos peritos externos relativas ao projeto de orientação. Indicou, porém, que tinha ocultado o nome desses peritos, de acordo com o artigo 4.º, n.º 1, alínea b), do Regulamento n.º 1049/2001 e com a legislação da União sobre proteção de dados pessoais, nomeadamente o Regulamento (CE) n.º 45/2001. Alegou, a esse respeito, que a divulgação do nome desses peritos correspondia a uma transferência de dados pessoais, na aceção do artigo 8.º do Regulamento (CE) n.º 45/2001, e que neste caso não estavam preenchidas as condições para essa transferência previstas no referido artigo.

Por conseguinte, a ClientEarth e a PAN Europe interpuseram recurso de anulação da referida decisão da EFSA no Tribunal Geral. O Tribunal Geral negou provimento ao recurso, tendo a ClientEarth e a PAN Europe interposto recurso do acórdão [34] do Tribunal Geral para o Tribunal de Justiça.

Em primeiro lugar, o Tribunal de Justiça salientou que, atendendo a que a informação pedida permitia relacionar um determinado perito com uma dada observação, a mesma dizia respeito a pessoas singulares identificadas e, portanto, constituía um conjunto de dados pessoais, na aceção do artigo 2.º, alínea a), do Regulamento (CE) n.º 45/2001. Dado que os conceitos de «dados pessoais», na aceção do artigo 2.º, alínea a), do Regulamento (CE) n.º 45/2001 e de «dados relativos à vida privada» não se confundem, o Tribunal de Justiça considerou, além disso, que a alegação da ClientEarth e da PAN Europe de que a informação em causa não estava abrangida pelo âmbito da vida privada desses peritos, era inoperante (n.os 29, 32).

O Tribunal de Justiça analisou em segundo lugar o argumento da ClientEarth e da PAN Europe baseado na existência de um clima de desconfiança em relação à EFSA, frequentemente acusada de parcialidade por recorrer a peritos com interesses pessoais ditados pelas suas ligações aos meios industriais, e na necessidade de garantir a transparência do processo decisório dessa autoridade. Este argumento baseava-se num estudo que fazia referências a ligações da maioria dos peritos que eram membros de um

32 Este acórdão foi apresentado no Relatório Anual de 2010, p. 14.

33 Regulamento (CE) n.º 1107/2009 do Parlamento Europeu e do Conselho, de 21 de outubro de 2009, relativo à colocação dos produtos fitofarmacêuticos no mercado e que revoga as Diretivas 79/117/CEE e 91/414/CEE do Conselho (JO L 309 de 24.11.2009, p. 1).

34 Acórdão do Tribunal Geral de 13 de setembro de 2013, ClientEarth e PAN Europe/EFSA (T-214/11, EU:T:2013:483).

grupo de trabalho da EFSA com organizações lobistas no domínio da indústria. A esse respeito, o Tribunal de Justiça declarou que a obtenção da informação controvertida era necessária para proceder à verificação concreta da imparcialidade de cada um desses peritos no desempenho da sua missão científica ao serviço da EFSA. Consequentemente, o Tribunal de Justiça anulou o acórdão do Tribunal Geral, declarando que foi erradamente que o Tribunal Geral considerou que este argumento da ClientEarth e da PAN Europe não bastava para demonstrar a necessidade da transferência da informação controvertida (n.os 57-59).

Em terceiro lugar, para apreciar a legalidade da decisão controvertida da EFSA, o Tribunal de Justiça examinou se existia ou não uma razão para pensar que a transferência podia ter lesado os interesses legítimos das pessoas em causa. A este respeito, constatou que a alegação da EFSA de que a divulgação da informação controvertida poderia causar prejuízo à vida privada e à integridade desses peritos era uma consideração de ordem geral não sustentada por nenhum elemento específico do caso vertente. O Tribunal de Justiça considerou, pelo contrário, que essa divulgação teria permitido, por si só, dissipar as suspeitas de parcialidade em causa ou teria dado aos peritos eventualmente afetados a oportunidade de contestarem, sendo caso disso pelos meios processuais disponíveis, o mérito dessas alegações de parcialidade. Atendendo a estes elementos, o Tribunal de Justiça anulou igualmente a decisão da EFSA (n.os 69, 73).

* * *

Os acórdãos que figuram na presente ficha são indexados no Repertório de Jurisprudência nas rubricas 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 e 4.11.07.